Christopher A. Seeger
Christopher Ayers
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, New Jersey 07660
(973) 639-9100
Quest Track Co-Lead Counsel
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: All Actions Against Quest Diagnostics, Inc. and Optum360 LLC	Civil Action No. 19-md-2904 (MCA)(MAH) **FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT: QUEST & OPTUM360**

TABLE OF CONTENTS

Page

Plaintiffs, individually and on behalf of a class of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiffs and on information and belief as to all other matters, and upon the investigation conducted by Plaintiffs' counsel, complain against Defendants, and allege on information and belief as follows:

PRELIMINARY STATEMENT

1. On June 3, 2019, Defendant Quest Diagnostics Inc. ("Quest") revealed in a securities filing that an unauthorized user accessed the system run by Quest's billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA"), for at least six months between late 2018 and March 2019 (the "Data Breach"). After accessing AMCA's unprotected systems, the malicious actors exfiltrated the sensitive personal, financial, and medical information (including physician names, tests ordered, and diagnosis codes that represent conditions and diseases) of millions of Quest patients, which was subsequently made available on the illegal marketplace known as the "dark web."

2. Quest contracted with AMCA through 2016 at which point Defendant Optum360 LLC ("Optum360") was assigned that contract pursuant to its work as a revenue cycle management company for Quest.

3. Defendants have a duty to safeguard and protect customer information entrusted to them and could have prevented this theft had they limited the customer information they shared with their vendors and business associates and employed reasonable measures to assure their vendors and business associates implemented and maintained adequate data security measures and protocols to secure and protect Quest customers' data.

4. Plaintiffs and Class Members entrusted Defendants with, and allowed Defendants to gather, highly sensitive information relating to their health and other matters as part of seeking

treatment. They did so in confidence, and they had the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it.

5. Trust and confidence are key components of Plaintiffs' and Class Members' relationship with Defendants. Without it, Plaintiffs and Class Members would not have provided Defendants with, or allowed Defendants to collect, their most sensitive information in the first place. To be sure, Plaintiffs and Class Members relied upon Defendants to keep their information secure, as they are required by law to do.

6. Plaintiffs bring this class action because Defendants collected and failed to secure and safeguard Quest patients' protected health information ("PHI") and personally identifiable information ("PII")—such as Plaintiffs' and Class Members' names, mailing addresses, phone numbers, email addresses, dates of birth, Social Security numbers, genders, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number), diagnosis codes, and other personal information—such as credit and debit card numbers, bank account information, and insurance policy numbers (all collectively referred to as "Personal Information").

7. As of today, more than 11.5 million Quest patients have had their Personal Information compromised as a result of the Data Breach. As a result of Defendants' failure to protect the consumer information they were entrusted to safeguard, Plaintiffs and Class Members suffered a loss of value of their Personal Information—and have been exposed to or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. In fact, many Class Members' identities have already been stolen.

8. Defendants' intentional, willful, reckless, unfair, and negligent conduct—failing to prevent the breach, failing to limit its severity, and failing to detect it in a timely fashion—harmed Plaintiffs uniformly. As discussed herein, fraudulent activities have already been linked to Defendants' unfair and deceptive conduct. For this reason, Defendants should pay for monetary damages, for appropriate identity theft protection services, and reimburse Plaintiffs for the costs caused by Quest's substandard security practices and failure to timely disclose the same. Plaintiffs are likewise entitled to injunctive and other equitable relief that safeguards their information, requires Defendants to significantly improve their data security, and provides independent, expert oversight of Defendants' security systems.

9. Defendants have also been unfairly and unjustly enriched as a result of their improper conduct, such that it would be inequitable for them to retain the benefits conferred upon them by Plaintiffs and the Class Members. Plaintiffs never would have engaged Quest to perform medical services and entrusted Defendants with their Personal Information, had they known that Defendants would permit unauthorized access to their Personal Information by Defendants' complete and utter disregard for security safeguards and protocols. Plaintiffs would have used another provider.

JURISDICTION AND VENUE

10. This Consolidated Complaint is intended to serve as an administrative summary as to all other complaints consolidated in this multidistrict litigation asserting claims against Quest and Optum360 and shall serve for all purposes as an administrative device to aid efficiency and economy for the Class defined below. As set forth herein, this Court has general jurisdiction over Defendants and original jurisdiction over Plaintiffs' claims.

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendants are citizens of States different from that of at least one Class member.

12. This Court has personal jurisdiction over Quest because it maintains its principal place of business in this District. Quest is authorized to and regularly conducts business in New Jersey. Quest makes decisions regarding corporate governance and management of its blood testing labs in this District, including decisions regarding the security measures to protect its customers' Personal Information. Quest owns and operates many blood testing labs throughout New Jersey and the United States.

13. This Court has personal jurisdiction over Optum360 because it is authorized and regularly conducts business in New Jersey and has sufficient minimum contacts in New Jersey such that Optum360 intentionally avails itself of this Court's jurisdiction by conducting operations here and contracts with companies in this District.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the July 31, 2019 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2904 or, in the alternative, pursuant to 28 U.S.C. § 1391 because each of the Defendants transact business and may be found in this District. Specifically, Quest's principal place of business is located in this District and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendants' governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach.

NAMED PLAINTIFFS

15. Plaintiffs are individuals who, upon information and belief, had their Personal Information compromised in the Data Breach, and bring this action on behalf of themselves and all those similarly situated both across the United States and within their state or territory of residence. These allegations are made upon information and belief derived from, *inter alia*, counsel's investigation, public sources—including sworn statements, Defendants' websites, and the facts and circumstances currently known. Because Defendants have exclusive but perhaps incomplete knowledge of what information was compromised for each individual, including PHI, Plaintiffs reserve the right to supplement their allegations with additional Plaintiffs, facts and injuries as they are discovered.

16. Each and every Plaintiff suffered a concrete and particularized injury as a result of Defendants' failure to protect their Personal Information and the subsequent disclosure of their Personal Information to unauthorized parties without their consent.

17. Had Defendants disclosed that they disregarded their duty to safeguard and protect Plaintiffs' Personal Information from unauthorized access, Plaintiffs would have taken them into account in making her healthcare decisions. In particular, had Plaintiffs known about Defendants' failure to ensure their vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' Personal Information, they would not have provided their Personal Information to Defendants and would have engaged a competing provider to perform medical services.

I. CALIFORNIA

A. Plaintiff Julio Antonio Perez Vieyra

18. Plaintiff Julio Antonio Perez Vieyra is a citizen and resident of California.

19. Plaintiff Vieyra was a Quest patient who went to a Quest laboratory to obtain blood testing services.

20. For years, Plaintiff Vieyra used Quest regularly for routine laboratory testing.

21. Plaintiff Vieyra reviewed and agreed to Quest's privacy policies prior to agreeing to obtain blood testing services.

22. Plaintiff Vieyra provided Quest with his Personal Information as part of obtaining blood testing, including his address, date of birth, Social Security number, and driver's license number.

23. Plaintiff Vieyra's bill from Quest was subsequently sent to AMCA.

24. In response to the Data Breach, Plaintiff Vieyra has begun carefully reviewing his financial and medical accounts to guard against fraud. Plaintiff Vieyra spends three hours every week monitoring his accounts for fraudulent activity.

25. In October 2019, Plaintiff Vieyra identified a fraudulent charge on his bank account and spent four hours attempting to contact his bank to alert them of the fraud.

26. Following the Data Breach, Plaintiff Vieyra began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Vieyra's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

27. As a Quest patient, Plaintiff Vieyra believed that Quest would protect his Personal Information once he provided it to Quest.

28. Plaintiff Vieyra would not have provided Quest with his Personal Information nor used Quest to provide blood testing had he known that it would fail to protect his Personal Information.

29. Plaintiff Vieyra suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Breanna Klein

30. Plaintiff Breanna Klein is a citizen and resident of California.

31. Plaintiff Klein was a Quest patient who went to a Quest laboratory to obtain laboratory services.

32. Plaintiff Klein reviewed Quest's privacy policies prior to agreeing to receiving laboratory services.

33. Plaintiff Klein provided Quest with her Personal Information as part of receiving laboratory services, including her address, date of birth, Social Security number, and driver's license number.

34. Plaintiff Klein's bill from Quest was subsequently sent to AMCA.

35. Following the Data Breach, Plaintiff Klein began receiving suspicious phishing text messages, emails and telephone calls. Plaintiff Klein's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

36. As a Quest patient, Plaintiff Klein believed that Quest would protect her Personal Information once she provided it to Quest.

37. Plaintiff Klein would not have provided Quest with Personal Information nor used Quest to provide laboratory services had she known that it would fail to protect her Personal Information.

38. Plaintiff Klein suffered and will continue to suffer damages due to the Data Breach.

C. Plaintiff Lisa Taylor

39. Plaintiff Lisa Taylor is a citizen and resident of California.

40. Plaintiff Taylor was a Quest patient who went to a Quest laboratory to obtain laboratory services.

41. Plaintiff Taylor provided Quest with her Personal Information as part of obtaining laboratory services.

42. Plaintiff Taylor's bill from Quest was subsequently sent to AMCA.

43. Plaintiff Taylor began regularly monitoring her financial accounts and obtained identify theft protection and credit monitoring services from Experian and McAfee after learning of the Data Breach.

44. Following the Data Breach, Plaintiff Taylor began receiving suspicious phishing telephone calls. Plaintiff Taylor's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

45. As a Quest patient, Plaintiff Taylor believed that Quest would protect her Personal Information once she provided it to Quest.

46. Plaintiff Taylor would not have provided Quest with Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

47. Plaintiff Taylor suffered and will continue to suffer damages due to the Data Breach.

II. FLORIDA

A. Plaintiff Noel Benadom

48. Plaintiff Noel Benadom is a citizen and resident of Florida.

49. Plaintiff Benadom was a Quest patient who went to a Quest laboratory to obtain blood testing services.

50. Plaintiff Benadom reviewed and agreed to Quest's privacy policies prior to agreeing to obtain blood testing services.

51. Plaintiff Benadom provided Quest with his Personal Information as part of obtaining blood testing.

52. Plaintiff Benadom's bill from Quest was subsequently sent to AMCA.

53. AMCA notified Plaintiff Benadom via letter dated June 4, 2019 of the Data Breach.

54. AMCA informed Plaintiff Benadom that information including his first and last name, his Social Security Number, the name of his lab or medical service provider, the date of his medical service, his referring doctor and other medical information may have been stored on AMCA's compromised system.

55. Following the Data Breach, on May 20, 2019, an unauthorized charge appeared on Plaintiff Benadom's Orbitz.com travel account due to unauthorized access.

56. On May 21, 2019, Orbitz.com confirmed that an unauthorized individual attempted to book a $125 ticket to Universal Studios Hollywood on Plaintiff Benadom's credit card.

57. Plaintiff Benadom spent more than one hour addressing the identity theft with Orbitz.com.

58. Plaintiff Benadom began regularly monitoring his financial accounts and obtained identify theft protection and credit monitoring services from Capital One and ID Me after learning of the Data Breach.

59. Following the Data Breach, Plaintiff Benadom began receiving suspicious phishing text messages. Plaintiff Benadom's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

60. As a Quest patient, Plaintiff Benadom believed that Quest would protect his Personal Information once he provided it to Quest.

61. Plaintiff Benadom would have sought an alternative medical testing facility had he known that Quest would not protect his Personal Information.

62. Plaintiff Benadom suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Nancy Infield

63. Plaintiff Nancy Infield is a citizen and resident of Florida.

64. Plaintiffs Infield is a Quest patient who went to a Quest laboratory to obtain blood testing services in at least 2013 and 2018.

65. Plaintiff Infield provided Quest with her Personal Information as part of obtaining blood testing.

66. Plaintiff Infield and her husband had unpaid bills from Quest, which were subsequently sent to AMCA.

67. Plaintiff Infield received three separate letters from AMCA, all dated June 6, 2019, informing her that her Personal Information including her "first and last name, Social Security number, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

68. In October 2019, Plaintiff Infield called AMCA and was told that the bill she was in collections for was owed to Quest.

69. Following the Data Breach, Plaintiff Infield began receiving suspicious phishing calls. The callers had her name, address, and last four digits of her Social Security number. She receives several calls per month. She has reported the calls to the Federal Trade Commission.

70. In response to the Data Breach, Plaintiff Infield took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

71. Plaintiff Infield believed that Quest would protect her Personal Information once she provided it to Quest.

72. Plaintiff Infield would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

73. Plaintiff Infield suffered and will continue to suffer damages due to the Data Breach.

C. Plaintiff Annie Mae Smith

74. Plaintiff Annie Mae Smith is a citizen and resident of Florida.

75. Plaintiff Smith was a Quest patient who went to a Quest laboratory to obtain blood testing services.

76. Plaintiff Smith provided Quest with her Personal Information as part of obtaining blood testing.

77. Plaintiff Smith's bill from Quest was subsequently sent to AMCA.

78. AMCA notified Plaintiff Smith of the Data Breach on June 4, 2019 and June 6, 2019.

79. AMCA informed Plaintiff Smith that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's compromised system.

80. Following the Data Breach, Plaintiff Smith began receiving suspicious phishing phone calls, text messages and emails. Plaintiff Smith's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

81. As a Quest patient, Plaintiff Smith believed that Quest would protect her Personal Information once she provided it to Quest.

82. Plaintiff Smith would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

83. Plaintiff Smith suffered and will continue to suffer damages due to the Data Breach.

D. Plaintiff Karen Copeland

84. Plaintiff Karen Copeland is a citizen and resident of Florida.

85. Plaintiff Copeland was a Quest patient who went to a Quest laboratory to obtain blood testing services and urinary analysis.

86. Plaintiff Copeland provided Quest with her Personal Information as part of obtaining blood testing and urinary analysis.

87. Plaintiff Copeland's bill from Quest was subsequently sent to AMCA.

88. Following the Data Breach, Plaintiff Copeland began receiving suspicious phishing text messages and emails. Plaintiff Copeland's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

89. In response to the Data Breach, Plaintiff Copeland took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity, and contacting the Internet Crime Complaint Center, the Federal Bureau of Investigation, and the Department of Justice.

90. As a Quest patient, Plaintiff Copeland believed that Quest would protect her Personal Information once she provided it to Quest.

91. Plaintiff Copeland would not have provided Quest with her Personal Information nor used Quest for testing had she known that it would fail to protect her Personal Information.

92. Plaintiff Copeland suffered and will continue to suffer damages due to the Data Breach.

III. INDIANA

A. Plaintiff Shannon Walden

93. Plaintiff Shannon Walden is a citizen and resident of Indiana.

94. Plaintiff Walden was a Quest patient who went to a Quest laboratory to obtain blood testing services in or about May 2018.

95. Plaintiff Walden provided Quest with her Personal Information as part of obtaining blood testing.

96. Plaintiff Walden's bill from Quest was subsequently sent to AMCA.

97. Plaintiff Walden received a notice of data breach from Quest Diagnostics and Optum 360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. The letter informed her that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

98. On or about July 23, 2019, Plaintiff Walden experienced identify theft after an unauthorized individual opened a Charles Schwab brokerage account in her name. Plaintiff Walden was informed that the account was opened using her name and/or Social Security number.

99. To attempt to resolve the identity theft issues caused by the Data Breach, Plaintiff Walden spent substantial time contacting Charles Schwab, the three major credit bureaus, and financial institutions where she held accounts.

100. In response to the Data Breach, Plaintiff Walden took measures to protect herself, including spending multiple hours monitoring her financial accounts and credit score for fraudulent activity, which she has continued to do.

101. Plaintiff Walden's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

102. Plaintiff Walden has experienced significant stress and anxiety from the Data Breach.

103. As a Quest patient, Plaintiff Walden believed that Quest would protect her Personal Information once she provided it to Quest.

104. Plaintiff Walden would not have provided Quest with her Personal Information nor used Quest for testing had she known that it would fail to protect her Personal Information.

105. Plaintiff Walden suffered and will continue to suffer damages due to the Data Breach.

106. As a Quest patient, Plaintiff Walden believed that Quest would protect her Personal Information once she provided it to Quest.

107. Plaintiff Walden would not have provided Quest with her Personal Information nor used Quest for testing had she known that it would fail to protect her Personal Information.

108. Plaintiff Walden suffered and will continue to suffer damages due to the Data Breach.

IV. IOWA

A. Plaintiff Lucinda Dirks

109. Plaintiff Lucinda Dirks is a citizen and resident of Iowa.

110. Plaintiff Dirks was a Quest patient who went to a Quest laboratory to obtain blood testing services.

111. Plaintiff Dirks provided Quest with her Personal Information as part of obtaining blood testing.

112. Plaintiff Dirks's bill from Quest was subsequently sent to AMCA.

113. AMCA notified Plaintiff Dirks via letter on June 4, 2019, of the Data Breach.

114. AMCA informed Plaintiff Dirks that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's compromised system.

115. In response to the Data Breach, Plaintiff Dirks has spent 40 hours monitoring her credit and financial accounts for fraudulent activity.

116. Following the Data Breach, Plaintiff Dirks began receiving suspicious phishing phone calls. Plaintiff Dirks's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

117. As a Quest patient, Plaintiff Dirks believed that Quest would protect her Personal Information once she provided it to Quest.

118. Plaintiff Dirks would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

119. Plaintiff Dirks suffered and will continue to suffer damages due to the Data Breach.

V. KANSAS

A. Plaintiff Ashley Finch

120. Plaintiff Ashley Finch is a citizen and resident of Kansas.

121. Plaintiff Finch has a chronic medical condition that requires quarterly diagnostic tests.

122. Plaintiff Finch was a Quest patient who went to a Quest laboratory to obtain blood testing services.

123. Plaintiff Finch has used Quest regularly since 2016.

124. Plaintiff Finch reviewed and agreed to Quest's privacy policies on an iPad prior to agreeing to obtain blood testing services.

125. Plaintiff Finch provided Quest with her Personal Information as part of obtaining blood testing.

126. Plaintiff Finch's bill from Quest was subsequently sent to AMCA.

127. Pursuant to a January 1, 2018 letter, AMCA sought to collect $108.24 from Plaintiff Finch on behalf of Quest.

128. AMCA notified Plaintiff Finch of the Data Breach in a letter dated June 4, 2019.

129. AMCA informed Plaintiff Finch that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's compromised system.

130. As a result of the Data Breach, Plaintiff Finch spends 10-20 minutes per week checking her credit report through Experian and Credit Karma.

131. Following the Data Breach, Plaintiff Finch began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Finch's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

132. As a Quest patient, Plaintiff Finch believed that Quest would protect her Personal Information once she provided it to Quest.

133. Plaintiff Finch would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

134. Plaintiff Finch suffered and will continue to suffer damages due to the Data Breach.

VI. KENTUCKY

A. Plaintiff Rose Marie Perry

135. Plaintiff Rose Marie Perry is a citizen and resident of Kentucky.

136. Plaintiff Perry was a Quest patient who went to a Quest laboratory to obtain blood testing services.

137. Plaintiff Perry provided Quest with her Personal Information as part of obtaining blood testing.

138. Plaintiff Perry's bill from Quest was subsequently sent to Defendants' billing collections vendor, AMCA.

139. Plaintiff Perry received a notice of data breach from Quest Diagnostics and Optum 360 dated July 8, 2019.

140. Plaintiff Perry's letter from Quest and Optum360 informed her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

141. In response to the Data Breach, Plaintiff Perry took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

142. Plaintiff Perry's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

143. As a Quest patient, Plaintiff Perry believed that Quest would protect her Personal Information once she provided it to Quest.

144. Plaintiff Perry would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

145. Plaintiff Perry suffered and will continue to suffer damages due to the Data Breach.

VII. MICHIGAN

A. Plaintiff Michael Rutan

146. Plaintiff Michael Rutan is a citizen and resident of Michigan.

147. Plaintiff Rutan was a Quest patient whose blood samples were sent to a Quest laboratory on multiple occasions over the past several years.

148. Plaintiff Rutan provided Quest with his Personal Information as part of obtaining blood testing services.

149. Plaintiff Rutan's bill from Quest was subsequently sent to AMCA.

150. Plaintiff Rutan received a letter from Quest and Optum360 dated July 8, 2019 informing him that his Personal Information was compromised in the Data Breach. It noted that the information at risk included his "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

151. Following the Data Breach, Plaintiff Rutan started receiving more frequent mailings for pre-approved credit cards, and an increased volume of robocalls.

152. In response to the Data Breach, Plaintiff Rutan took mitigative measures, including spending substantial time monitoring his accounts for fraudulent activity.

153. Following the Data Breach, Plaintiff Rutan began receiving suspicious phishing emails, text messages, and phone calls. Plaintiff Rutan's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

154. As a Quest patient, Plaintiff Rutan believed that Quest would protect his Personal Information once it was provided to Quest.

155. Plaintiff Rutan would not have provided Quest with this Personal Information nor used Quest to provide blood testing had he known that it would fail to protect his Personal Information.

156. Plaintiff Rutan suffered and will continue to suffer damages due to the Data Breach.

VIII. MINNESOTA

A. Plaintiff Elizabeth Hollway

157. Plaintiff Elizabeth Hollway is a citizen and resident of Minnesota.

158. Plaintiff Hollway was a Quest patient who went to a Quest laboratory to obtain blood testing services on, among other dates, May 8, 2018, June 22, 2018, and August 1, 2018.

159. Plaintiff Hollway reviewed and agreed to Quest's privacy policies on an iPad prior to agreeing to obtain blood testing services.

160. Plaintiff Hollway provided Quest with her Personal Information as part of obtaining blood testing.

161. Plaintiff Hollway's bill from Quest was subsequently sent to AMCA.

162. Plaintiff Hollway paid Quest for the testing services on August 1, 2018.

163. Plaintiff Hollway paid AMCA for Quest's services on January 8, 2019.

164. AMCA notified Plaintiff Hollway via letter on June 4, 2019 of the Data Breach.

165. In that letter, AMCA informed Plaintiff Hollway that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's compromised system.

166. Following the Data Breach, on June 10, 2019 Plaintiff Hollway experienced unauthorized charges on her credit card.

167. On June 10, 2019, an unauthorized individual purchased a $200 restaurant gift card using Plaintiff Hollway's Personal Information.

168. Plaintiff Hollway also experienced identify theft: an unauthorized individual opened a Nordstrom credit card in her name as a result of the Data Breach.

169. Plaintiff Hollway was informed that whoever opened the Nordstrom account provided Nordstrom with her name, Social Security number, and date of birth.

170. To attempt to resolve the identity theft issues caused by the Data Breach, Plaintiff Hollway spent 15 hours contacting Transunion, Equifax, Experian, her mortgage companies and banks where she held accounts, credit cards, and debit cards.

171. Additionally, to attempt to resolve the issues, Plaintiff Hollway purchased a monthly subscription to Lifelock for identity theft protection for $31.96 per month.

172. Following the Data Breach, Plaintiff Hollway began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Hollway's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

173. As a Quest patient, Plaintiff Hollway believed that Quest would protect her Personal Information once she provided it to Quest.

174. Plaintiff Hollway would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

175. Plaintiff Hollway suffered and will continue to suffer damages due to the Data Breach.

IX. MISSOURI

A. Plaintiff LaTease Rikard

176. Plaintiff LaTease Rikard is a citizen and resident of Missouri.

177. Plaintiff Rikard was a Quest patient who went to a Quest laboratory to obtain blood testing services several times in the past few years.

178. Plaintiff Rikard provided Quest with her Personal Information as part of obtaining blood testing.

179. Plaintiff Rikard's bill from Quest was subsequently sent to AMCA.

180. Plaintiff Rikard received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

181. In response to the Data Breach, Plaintiff Rikard took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

182. Following the Data Breach, Plaintiff Rikard began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Rikard's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

183. As a Quest patient, Plaintiff Rikard believed that Quest would protect her Personal Information once she provided it to Quest.

184. Plaintiff Rikard would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

185. Plaintiff Rikard suffered and will continue to suffer damages due to the Data Breach.

X. NEW HAMPSHIRE

A. Plaintiff Naomi Jaworowski

186. Plaintiff Naomi Jaworowski is a citizen and resident of New Hampshire.

187. Plaintiff Jaworowski was a Quest patient who went to a Quest laboratory to obtain blood testing services approximately two years ago.

188. Plaintiff Jaworowski provided Quest with her Personal Information as part of obtaining blood testing.

189. Plaintiff Jaworowski's bill from Quest was subsequently sent to AMCA.

190. Plaintiff Jaworowski received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers

and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

191. In response to the Data Breach, Plaintiff Jaworowski called the Attorney General's Office to ask how she can protect herself. She also called Quest for more information about the breach. She also took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

192. Following the Data Breach, Plaintiff Jaworowski began receiving suspicious phishing emails and text messages. Plaintiff Jaworowski's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

193. As a Quest patient, Plaintiff Jaworowski believed that Quest would protect her Personal Information once she provided it to Quest.

194. Plaintiff Jaworowski would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

195. Plaintiff Jaworowski suffered and will continue to suffer damages due to the Data Breach.

XI. NEW JERSEY

A. Plaintiff Ria Jairam

196. Plaintiff Ria Jairam is a citizen and resident of New Jersey.

197. Plaintiff Jairam was a Quest patient who went to a Quest laboratory to obtain blood testing services.

198. Plaintiff Jairam provided Quest with her Personal Information as part of obtaining blood testing.

199. Plaintiff Jairam's bill from Quest was subsequently sent to AMCA.

200. Plaintiff Jairam received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

201. Plaintiff Jairam suffered identify theft as a result of the Data Breach.

202. Following the Data Breach, Plaintiff Jairam's Chase Bank account was compromised and $2,000 was fraudulently withdrawn. As a result, Plaintiff Jairam had to close her bank accounts and cancel her credit cards.

203. Plaintiff Jairam was informed by Navy Federal Credit Union of additional possible fraudulent activity requiring new bank accounts to be opened.

204. To attempt to resolve the identity theft issues caused by the Data Breach, Plaintiff Jairam spent 12 hours reviewing her bank accounts as a result of these fraudulent activities.

205. Following the Data Breach, Plaintiff Jairam began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Jairam's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

206. As a Quest patient, Plaintiff Jairam believed that Quest would protect her Personal Information once she provided it to Quest.

207. Plaintiff Jairam would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

208. Plaintiff Jairam suffered and will continue to suffer damages due to the Data Breach.

XII. NEW YORK

A. Plaintiff John Briley

209. Plaintiff John Briley is a citizen and resident of New York.

210. Plaintiff Briley was a Quest patient who went to a Quest laboratory to obtain blood testing in at least the past two to three years.

211. Plaintiff Briley provided Quest with his Personal Information as part of obtaining blood testing.

212. Plaintiff Briley's bill from Quest was subsequently sent to AMCA.

213. Plaintiff Briley received a letter from Quest and Optum360 dated July 8, 2019 informing him that his Personal Information was compromised in the Data Breach. It noted that the information at risk included his "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

214. His eighteen-year-old daughter received a similar letter from Quest dated July 8, 2019 regarding blood testing services she obtained under his insurance plan.

215. Plaintiff Briley received a letter from TD Bank dated October 2, 2019 regarding a fraudulent "application for an account with Samsung Financing." An imposter attempted to open the account using a false name and Plaintiff Briley's mailing address.

216. Plaintiff Briley had not experienced any similar fraudulent activity prior to the Data Breach.

217. In response to the Data Breach, Plaintiff Briley took mitigative measures, including spending substantial time monitoring his accounts for fraudulent activity.

218. Following the Data Breach, Plaintiff Briley began receiving suspicious phishing phone calls. Plaintiff Briley's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

219. As a Quest patient, Plaintiff Briley believed that Quest would protect his Personal Information once he provided it to Quest.

220. Plaintiff Briley would not have provided Quest with this Personal Information nor used Quest to provide blood testing had he known that it would fail to protect his Personal Information.

221. Plaintiff Briley suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Karli Parker

222. Plaintiff Karli Parker is a citizen and resident of New York.

223. Plaintiff Parker was a Quest patient who went to a Quest laboratory to obtain blood testing services.

224. Plaintiff Parker provided Quest with her Personal Information as part of obtaining blood testing.

225. Plaintiff Parker's bill from Quest was subsequently sent to AMCA.

226. Plaintiff Parker received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

227. In response to the Data Breach, Plaintiff Parker took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

228. Following the Data Breach, Plaintiff Parker began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Parker's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

229. As a Quest patient, Plaintiff Parker believed that Quest would protect her Personal Information once she provided it to Quest.

230. Plaintiff Parker would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

231. Plaintiff Parker suffered and will continue to suffer damages due to the Data Breach.

C. Plaintiff Joyce Rosselli

232. Plaintiff Joyce Rosselli is a citizen and resident of New York.

233. Plaintiff Rosselli was a Quest patient who went to a Quest laboratory to obtain blood testing services several times over the last few years.

234. Plaintiff Rosselli provided Quest with her Personal Information as part of obtaining blood testing.

235. Plaintiff Rosselli's bill from Quest was subsequently sent to AMCA.

236. On June 4, 2019, Plaintiff Rosselli received a letter from AMCA informing her that her Personal Information including her "first and last name, Social Security number, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

237. In response to the Data Breach, Plaintiff Rosselli signed up for the free two-year credit monitoring service offered by AMCA.

238. In further response to the Data Breach, on June 17, 2019, Plaintiff Rosselli placed a "fraud alert" on her credit report.

239. In response to the Data Breach, Plaintiff Rosselli took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

240. Plaintiff Rosselli received an alert from her Capital One CreditWise fraud monitoring product stating that her email address was found on the dark web on June 8, 2019 and July 6, 2019. Those dates were several months after threat actors are known to have first accessed AMCA's system.

241. On or around July 11, 2019, Plaintiff Rosselli called Quest's data breach hotline to determine whether her involvement in the Data Breach was related to Quest. The Quest representative confirmed that her involvement in the breach was related to Quest.

242. Following the Data Breach, Plaintiff Rosselli began receiving suspicious phishing emails from strangers requesting her account information.

243. As a Quest patient, Plaintiff Rosselli believed that Quest would protect her Personal Information once she provided it to Quest.

244. Plaintiff Rosselli would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

245. Plaintiff Rosselli suffered and will continue to suffer damages due to the Data Breach.

XIII. OHIO

A. Plaintiff Deanna Taylor

246. Plaintiff Deanna Taylor is a citizen and resident of Ohio.

247. Plaintiff Taylor was a Quest patient who obtained blood testing through Quest.

248. Plaintiff Taylor provided Quest with her Personal Information as part of obtaining blood testing.

249. Plaintiff Taylor's bill from Quest was subsequently sent to AMCA.

250. In November 2019, Plaintiff Taylor called Quest's data breach hotline to verify that she was involved in the Data Breach. The Quest representative confirmed that she was involved in the Data Breach.

251. In response to the Data Breach, Plaintiff Taylor took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

252. Following the Data Breach, Plaintiff Taylor began receiving suspicious phishing phone calls, emails, and text messages.

253. As a Quest patient, Plaintiff Taylor believed that Quest would protect her Personal Information once she provided it to Quest.

254. Plaintiff Taylor would not have provided Quest with this Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

255. Plaintiff Taylor suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Matthew DiFonzo

256. Plaintiff Matthew DiFonzo is a citizen and resident of Ohio.

257. Plaintiff DiFonzo was a Quest patient who went to a Quest laboratory to obtain laboratory services.

258. Plaintiff DiFonzo provided Quest with his Personal Information as part of obtaining laboratory services.

259. Plaintiff DiFonzo's bill from Quest was subsequently sent to AMCA.

260. Plaintiff DiFonzo began regularly monitoring his financial accounts and obtained identify theft protection and credit monitoring services from LifeLock after learning of the Data Breach.

261. Following the Data Breach, Plaintiff DiFonzo began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff DiFonzo's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

262. As a Quest patient, Plaintiff DiFonzo believed that Quest would protect his Personal Information once he provided it to Quest.

263. Plaintiff DiFonzo would not have provided Quest with his Personal Information nor used Quest for testing had he known that it would fail to protect his Personal Information.

264. Plaintiff DiFonzo suffered and will continue to suffer damages due to the Data Breach.

XIV. PENNSYLVANIA

A. Plaintiff Brittney Petitta

265. Plaintiff Brittney Petitta is a citizen and resident of Pennsylvania.

266. Plaintiff Petitta was a Quest patient who went to a Quest laboratory to obtain blood testing services in at least 2018.

267. Plaintiff Petitta provided Quest with her Personal Information as part of obtaining blood testing.

268. Plaintiff Petitta's bill from Quest was subsequently sent to AMCA.

269. Plaintiff Petitta received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

270. In response to the Data Breach, Plaintiff Petitta took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

271. Following the Data Breach, Plaintiff Petitta began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Petitta's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

272. As a Quest patient, Plaintiff Petitta believed that Quest would protect her Personal Information once she provided it to Quest.

273. Plaintiff Petitta would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

274. Plaintiff Petitta suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Darlane Saracina

275. Plaintiff Darlane Saracina is a citizen and resident of Pennsylvania.

276. Plaintiff Saracina was a Quest patient who went to a Quest laboratory to obtain blood testing services several times over the last few years.

277. Plaintiff Saracina provided Quest with her Personal Information as part of obtaining blood testing.

278. Plaintiff Saracina's bill from Quest was subsequently sent to AMCA.

279. Plaintiff Saracina received a letter from Quest in or around July 2019 informing her that her Personal Information was at risk due to the Data Breach.

280. On October 10, 2019, Plaintiff Saracina also called the Quest data breach hotline to confirm that her involvement in the Data Breach was related to Quest. The Quest representative verified that her involvement in the breach was related to Quest.

281. Plaintiff Saracina received an alert from her Capital One CreditWise fraud monitoring product stating that her Social Security number was found on the dark web on September 25, 2018.

282. In or about June 2021, Plaintiff Saracina received notification from the Pennsylvania Department of Labor and Industry Office of Unemployment Compensation Benefits

that her claim for unemployment benefits was denied. Plaintiff Saracina never filed for unemployment benefits, so she immediately contacted the Office of Unemployment and was instructed to submit an identity theft complaint through its Fraud Reporting System.

283. To attempt to resolve the identity theft issues caused by the Data Breach, Plaintiff Saracina spent substantial time working with the Office of Unemployment to address the fraudulent claim, which was not fully resolved until almost a year later.

284. As a further result of the Data Breach, on or about September 24, 2021, Plaintiff Saracina became aware of a $1.00 charge on her account with Credit One Bank, N.A. to an unknown PayPal account. Plaintiff Saracina successfully disputed the charge shortly thereafter. Plaintiff Saracina believes this charge was an attempt by an unauthorized person to gain access to her account.

285. In response to the Data Breach, Plaintiff Saracina took mitigative measures, including spending substantial time monitoring her accounts and fraud monitoring service for fraudulent activity.

286. Following the Data Breach, Plaintiff Saracina began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Saracina's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

287. As a Quest patient, Plaintiff Saracina believed that Quest would protect her Personal Information once she provided it to Quest.

288. Plaintiff Saracina would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

289. Plaintiff Saracina suffered and will continue to suffer damages due to the Data Breach.

XV. TENNESSEE

A. Plaintiff Jo Ann Buck

290. Plaintiff Jo Ann Buck is a citizen and resident of Tennessee.

291. Plaintiff Buck was a Quest patient who went to a Quest laboratory to obtain blood testing services within the past few years.

292. Plaintiff Buck provided Quest with her Personal Information as part of obtaining blood testing.

293. Plaintiff Buck's bill from Quest was subsequently sent to AMCA.

294. Plaintiff Buck received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

295. On December 27, 2021, Plaintiff Buck received a notification from her bank informing her that someone made two fraudulent charges using the same debit card she provided to Defendants and AMCA.

296. In response to the Data Breach, Plaintiff Buck took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

297. Following the Data Breach, Plaintiff Buck began receiving suspicious phishing phone calls and emails. Plaintiff Buck's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

298. As a Quest patient, Plaintiff Buck believed that Quest would protect her Personal Information once she provided it to Quest.

299. Plaintiff Buck would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

300. Plaintiff Buck suffered and will continue to suffer damages due to the Data Breach.

XVI. TEXAS

A. Plaintiff Ann Davis

301. Plaintiff Ann Davis is a citizen and resident of Texas.

302. Plaintiff Davis was a Quest patient who went to a Quest laboratory to obtain blood testing at least once per year for the past several years.

303. Plaintiff Davis provided Quest with her Personal Information as part of obtaining blood testing services.

304. Quest sent multiple bills of Plaintiff Davis's to collections. At least one such bill was sent to AMCA.

305. Plaintiff Davis received a letter from AMCA dated June 4, 2019 informing her that her Personal Information including her "first and last name, Social Security Number, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

306. In or around early 2019, Plaintiff Davis received a call from her credit card company stating that someone charged $800 for a fraudulent purchase at Boost Mobile. The credit

card company issued her a replacement card. Plaintiff Davis believes the compromised card was the same card she used to pay Quest bills.

307. In response to the Data Breach, Plaintiff Davis took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity. She spends one to two hours per week checking her accounts. She also spent approximately two hours in connection with the credit card fraud.

308. Plaintiff Davis also purchased a new antivirus product due at least in part to her fear of harm from the Data Breach.

309. Following the Data Breach, Plaintiff Davis began receiving suspicious phishing phone calls, emails, and text messages. Plaintiff Davis's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

310. As a Quest patient, Plaintiff Davis believed that Quest would protect her Personal Information once she provided it to Quest.

311. Plaintiff Davis would not have provided Quest with this Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

312. Plaintiff Davis suffered and will continue to suffer damages due to the Data Breach.

DEFENDANTS

313. Quest Diagnostics Incorporated is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

314. Optum360, LLC is a Delaware limited liability company with its principal place of business in Eden Prairie, Minnesota.

FACTUAL ALLEGATIONS

A. Quest's Data Protection Obligations

315. Quest markets itself as "the world's leading provider of diagnostic information services." Quest's operations are national in scope and the company purports to annually serve one in three adult Americans and half the physicians and hospitals in the United States. Quest generated revenues of approximately $9.44 billion in 2020, up 22% from the prior year alone.

316. Quest's business operations include operating over 2,250 "Patient Service Centers" where patient's blood is drawn and tested following an order from a doctor.[1] Quest's clinical laboratory testing includes blood tests, body fluid testing, tissue pathology and cytology, health screening and monitoring tests, drug screening and testing as well as gene-based testing (genetic testing).[2] Quest's blood tests relate to a wide array of medical conditions, including but not limited to: allergy and asthma, human immunodeficiency virus ("HIV"), ovarian, breast and other cancer screening, hepatitis C, and prenatal health screening.

317. Quest states that it "obtains diagnosis information from the ordering physicians [sic] office."[3] Quest also asks its patients to bring photo identification, current health insurance information, and permits alternative methods of payment for costs in excess or beyond the scope of the patient's insurance and if the patient is uninsured.[4]

---

[1] https://www.questdiagnostics.com/patients/get-tested/prepare (last visited March 21, 2022).

[2] *Id.*

[3] Quest Diagnostics, Frequently Asked Questions: Billing Services, "Where does Quest Diagnostics obtain the diagnosis information related to my claim?" https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq (last visited March 21, 2022).

[4] https://www.questdiagnostics.com/patients/get-tested/prepare (last visited March 21, 2022).

318. Quest's contracts with its patients and policies on its website commit it to protecting patient information, including information shared with third parties.

319. Quest's website makes it clear that it will protect payment information. In response to the question "Is my payment information secure" on its facts and questions page, Quest unequivocally states "yes."[5] Quest promises "Transport Security Layer (TSL) to encrypt your credit card number, name, and address information so only QuestDiagnostics.com is able to decode your information."[6]

320. Quest's privacy policy states that the disclosure of personal information to third parties is limited to "contractors to who we may provide such information for the limited purpose of providing services to us ***and who are obligated to keep the information confidential***."[7]

321. Quest's privacy policy assures that "we limit Quest Diagnostics' employees and contractors' access to personal information. Only those employees and contractors with a business reason to know have access to this information."[8]

322. Quest also has an Online Privacy Policy where it makes additional promises to its customers regarding the privacy of their Sensitive Information:

> **How We Protect Information Online**
>
> We exercise great care to protect your personal information. This includes, among other things, using industry standard techniques such as firewalls, encryption, and intrusion detection. As a result, while we strive to protect your personal information, we cannot ensure or warrant the security of any information you transmit to us or receive from us. This is especially true for information you

[5] Quest Diagnostics, https://myquest.questdiagnostics.com/myquest-faq1/QuestDirect.htm (last visited Mar. 21, 2022).

[6] *Id.*

[7] Online Privacy Policy, https://web.archive.org/web/20190925091329/https://www.questdiagnostics.com/home/privacy-policy/online-privacy.html (last visited Mar. 21, 2019) (emphasis added).

[8] *Id.*

> transmit to us via email since we have no way of protecting that information until it reaches us since email does not have the security features that are built into our websites.
>
> In addition, we limit Quest Diagnostics' employees and contractors' access to personal information. Only those employees and contractors with a business reason to know have access to this information. We educate our employees about the importance of maintaining confidentiality of customer information.
>
> ***
>
> **Disclosure of Personal Information to Third Parties**
> We will not disclose any personal information to any third party (excluding our contractors to whom we may provide such information for the limited purpose of providing services to us and who are obligated to keep the information confidential), unless (1) you have authorized us to do so; (2) we are legally required to do so, for example, in response to a subpoena, court order or other legal process and/or, (3) it is necessary to protect our property rights related to this website. We also may share aggregate, non-personal information about website usage with unaffiliated third parties. This aggregate information does not contain any personal information about our users.

323. Quest and its affiliates have a non-delegable duty under federal law to ensure that all information they collect and store is secure, and that any associated entities with whom they shared information maintain adequate and commercially reasonable data security practices to ensure the protection of patients' Personal Information.

324. Indeed, Quest's entire business depends on patients entrusting it with their Personal Information. Without patients' Personal Information, Quest would not be able to perform any services and certainly would not be able to bill patients and their insurance companies and collect payment for services rendered. More specifically, to provide services to patients, Quest knows that its patients must trust that Quest is keeping their health information private and secure. If Quest's patients lack trust in Quest or knew Quest would insecurely store, safeguard, or transmit their personal information, then they will not disclose health information to it and will choose a different provider for services.

325. More specifically, to provide services to patients, Quest and patients must trust that the patients' health information is private and secure. If Quest's patients lack trust in Quest or knew Quest would insecurely store, safeguard, or transmit their personal information or failed establish or follow data security policies and protocols, they will not disclose health information to it and will choose a different provider for services.

326. This is why Quest is an entity covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), *see* 45 C.F.R. § 160.102, and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

327. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

328. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

329. HIPAA requires that Quest implement appropriate safeguards for this information.

330. HIPAA also requires that Quest provide every patient it treats, including Plaintiffs and the putative Class Members with a privacy notice. Quest's "Notice of Privacy Practices" acknowledges their legal requirement to maintain the privacy of patients' PHI, and states it is "are

committed to protecting the privacy of your identifiable health information."[9] Quest states that "we are required notify affected individuals in the event of a breach involving unsecured protected health information."[10]

331. Quest's Notice of Privacy Policies indicates that it may provide PHI to companies that assist with billing and to "an outside collection agency to obtain payment when necessary."[11] These "business associates" are "***required to maintain the privacy and security of PHI***."[12]

332. HIPAA mandates that a covered entities such as Quest may disclose PHI to a "business associate," only if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[13]

333. HIPAA further requires that Quest provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – i.e. non-encrypted data.

B. Quest Collects Patients' Personal Information and Shares it with Optum360 and AMCA

334. Quest's invoices cover laboratory testing fees only and are separate from any bill received by a patient's physician. Patients can be charged following an in-person visit to a Quest

[9] Notice of Privacy Practices, https://web.archive.org/web/20190606194629/https://www.questdiagnostics.com/dms/Documents/Other/privacy-policy/qd-notice-of-privacy-practices-04-07-2014/Notice-of-Privacy-Practices_Eng_100215.pdf (last visited Mar. 21, 2022).

[10] *Id.*

[11] *Id.*

[12] *Id.* (emphasis added).

[13] *See* 45 CFR §§ 164.502(e), 164.504(e), 164.532(d) and (e).

Patient Service Center or when their physician sends their specimen to a Quest Diagnostics laboratory.[14] Patients are responsible for paying Quest for performing diagnostic services either through their insurance or out-of-pocket where the patient does not have insurance or the costs are not covered in whole or part.

335. If Quest does not receive payment within a specified time period, Quest employs an associated business for collection. Prior to September 2016, Quest's collection agent by contract or direct association was AMCA. In September 2016, Quest partnered with Optum360 so that Quest's revenue services operations would become part of Optum360.[15] Thereafter, Quest assigned its contract with AMCA to Optum360 and AMCA delivered Quest's outstanding invoices, including Quest patients' Personal Information, to AMCA.[16] Before and after Quest assigned its contract to Optum360, Quest provided its patients' Personal Information directly to AMCA.

336. In order to facilitate collection, Quest and Optum360 would send daily "placement" files of allegedly delinquent accounts to AMCA containing the name, address, date of birth, and Social Security numbers of Quest patients as a matter of course. Quest and Optum360 would also regularly transfer additional information to AMCA for purposes of addressing billing questions, collection disputes, and credit reporting issues. This information included insurance information,

[14] Quest Diagnostics, Frequently Asked Questions: Billing Services, "Why have I received a bill from Quest Diagnostics?" https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq (last visited Mar. 21, 2022).

[15] Optum and Quest Diagnostics Partner to Help Make the Health System Work Better for Patients, Physicians, Health Plans and Employers, Sept. 13, 2016, https://www.optum.com/about/news/optum-quest-diagnostics-partner-help-make-health-system-work-better-for-patients-physicians-health-plans-employers.html (last visited Mar. 21, 2022).

[16] Quest Diagnostics Incorporated, 2018 Annual Report (Form 10-K), at 58.

the name of their employer (if the test was part of their employment), and protected health information under HIPAA, including patient information in conjunction with the referring physician's name and International Classification of Diseases Diagnosis and Procedure Codes ("ICD Codes"),[17] which are defined by the Centers for Disease Control and Prevention ("CDC") as "the official system of assigning codes to diagnoses and procedures associated with hospital utilization in the United States."[18]

337. ICD Codes are assigned to every disease and used to relay and track conditions and diseases in a standardized fashion. The CDC refers to ICD Codes as "the cornerstone of classifying diseases, injuries, health encounters and inpatient procedures in morbidity settings. U.S. public health officials at the federal, state, and local level rely on the receipt of ICD-9-CM coded data from HIPAA-covered entities to conduct many disease-related activities."[19] The CDC notes that:

- **A primary user** of ICD codes includes health care personnel, such as physicians and nurses, as well as medical coders, who assign ICD-9-CM codes to verbatim or abstracted diagnosis or procedure information, and thus are originators of the ICD codes. ICD-9-CM codes are used for a variety of purposes, including statistics and for billing and claims reimbursement.

- **A secondary user** of ICD-9-CM codes is someone who uses already coded data from hospitals, health care providers, or health plans to conduct surveillance and/or research activities. Public health is largely a secondary user of coded data.[20]

---

[17] The ICD has been revised periodically to incorporate changes in the medical field and many stakeholders have transitioned from the Ninth Revision (ICD-9) to the Tenth Revision (ICD-10). It appears that Quest used ICD-9 coding as of the time of the breach.

[18] Centers for Disease Control and Prevention, International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM), https://www.cdc.gov/nchs/icd/icd9cm.htm#:~:text=ICD%2D9%2DCM%20is%20the,10%20for%20mortality%20coding%20started (last visited Mar. 21, 2022).

[19] Centers for Disease Control and Prevention, International Classification of Diseases, (ICD-10-CM/PCS) Transition - Background, https://www.cdc.gov/nchs/icd/icd10cm_pcs_background.htm (last visited Mar. 21, 2022).

[20] *Id*.

338. ICD Codes can be used to identify information relating to an individual's medical history, mental or physical condition, and treatment. Indeed, there are numerous publicly available online databases that allow anyone with an internet connection to quickly and easily look up specific diagnosis or condition information associated with an ICD Code.[21] Accounting for the specificity reflected in the coding process, the most recent revision of the ICD Code contains more than 72,000 diagnosis codes that represent conditions and diseases, related health problems, abnormal findings, signs and symptoms, injuries, external causes of injuries and diseases, and social circumstances.[22] For example, ICD-9-CM Code 042 means a conclusive diagnosis of symptomatic HIV infection. ICD-9-CM Code 795.71 means inconclusive or nonspecific HIV test results, including inconclusive HIV test findings in infants. ICD-9-CM Code 054.9 means a diagnosis of herpes simplex without mention of complication, while ICD-9-CM Code 054.11 means herpetic infection of the penis.

339. The methods of transmission of information between Quest and AMCA varied by Quest division. For example, from 2014 through 2019, Solstas Lab Partners, a diagnostic company acquired by Quest in 2014, emailed Excel files to AMCA that included hundreds of patient names, addresses, dates of birth, and Social Security numbers. Security protocols were lax as oftentimes the password needed to access the file was listed in the in the body of the email. These files were then forwarded without passwords and stored on AMCA's servers, which AMCA referred to as "Live files."

[21] *See, e.g.*, ICD Code Lookup, https://icdcodelookup.com/icd-10/codes; ICD10Data.com, https://www.icd10data.com/; Codify by AAPC, https://www.aapc.com/codes/icd-10-codes-range/.

[22] Codify by AAPC, What is ICD-10?, https://www.aapc.com/icd-10/ (last visited Mar. 21, 2022).

340. Other Quest divisions had direct access to AMCA's network, which allowed Quest and Optum360 to upload files directly onto folders stored on AMCA's "O drive." This transfer method was extremely unsecure and AMCA internally acknowledged it posed "a serious security risk." Nevertheless, Quest resisted adopting a more secure file transfer method because of the ease of the data transfer process.

341. In many instances, Quest and Optum360 employees would simply email patient account information directly to AMCA, including, by default, patient names, addresses, billing codes, physician names, and ICD Codes, among other highly sensitive information.

342. During its bankruptcy proceedings in the U.S. Bankruptcy Court in the Southern District of New York, AMCA admitted that its "business, by its very nature, requires it to collect and maintain data transmitted to it by its clients [such as Quest] that includes personally identifiable information about third-party debtors that could include names, home addresses, Social Security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information." AMCA also admitted that this "information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought."[23]

343. In addition, as part of AMCA's billing collection services for Defendants, Plaintiffs furnished Personal Information to AMCA, which AMCA subsequently stored.

C. How the Data Breach Occurred

344. From at least August 1, 2018 through March 30, 2019, an unauthorized user or users gained access to the AMCA system that contained information obtained from various entities,

[23] Decl. of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions, *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 19-23185-RDD (Bankr. S.D.N.Y. June 17, 2019), ECF No. 2 at 4-5.

including Defendant Quest, as well as information that AMCA collected itself. [redacted] and the intrusion may have covered a longer period.

345. Upon information and belief, and based on the limited documents produced to date, the threat actors were able to exploit easily-recognizable vulnerabilities in the AMCA IT infrastructure to perpetrate the Data Breach.

[redacted]

347. [redacted]

348. Specifically, the evidence shows that [redacted].[25] Web shells are pieces of code placed on a web application server to provide an interface for a remote attacker to execute commands. An attacker attaches an executable script, here [redacted], to the web server and the script

[24] [redacted] (emphasis added).

[25] *Id.*

searches for vulnerabilities in a web server's systems. The web shell can also execute commands and upload and download files.

349. Web shells are only possible if the web application or server contain vulnerabilities such as insecure or poorly written code, a misconfiguration, credentials that are unencrypted, a lack of security patching, or minimal segmentation between different areas in a network. Moreover, web shells leave contemporaneous evidence of their activities, referred to as "noise,"

Additionally, commercial scanning tools and anti-virus software can detect and prevent the installation of web shells,

351. Specifically, threat actors found the following :[26]

a. ;

b. ;

[26] RMCB-AG-195, at 3-4.

[redacted] In March 2020, amcaonline.com still showed an unpatched version of Apache and an unpatched version of MySQL.

353. [redacted] This is a basic feature of IT security. It is well known in the industry that threat actors learn of vulnerabilities in IT systems and exploit them if they are not patched, and even basic IT security requires constant patching and updating as potential vulnerabilities become known. [redacted]

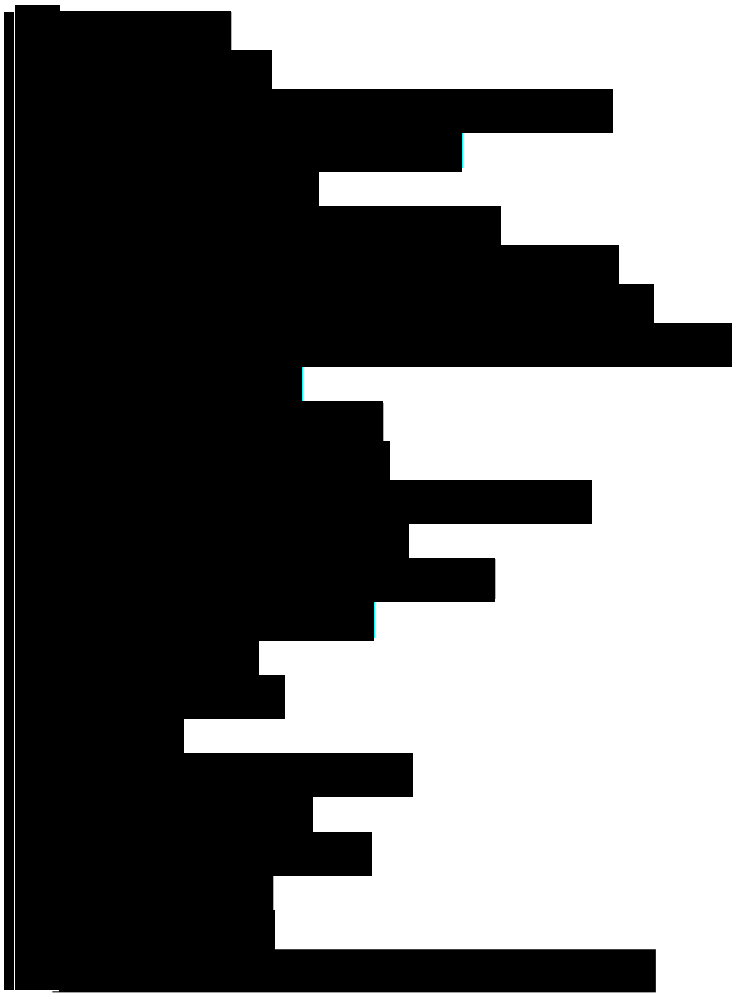
354. As a result, AMCA's system was not a difficult system to attack; threat actors could have discovered the vulnerabilities through simple open-source tools from the Internet and commercially available hacking tools.

355. Once threat actors were inside AMCA's systems, they were not detected in part because:

[redacted]

[redacted] Even if an attacker is able to get into AMCA's systems via a webshell, an appropriate IT system needs to provide additional security to protect the most important (and desirable) information. This includes taking steps to segregate the most important systems from

the rest of the system and limiting who can access these systems. [redacted]



[redacted]

[redacted]

359. [redacted][27]

360. [redacted]

362. [redacted]

363. At no point did AMCA discover the threat actors—not upon entry, not when they traversed the system, not when they overrode the requirement for a user to authenticate themselves, and not when they exfiltrated files.

[27] [redacted].

D. AMCA's 2019 Audit Revealed Serious Vulnerabilities That It Did Not Remediate

[redacted] In layman's terms, this meant that compromising the public-facing web server allowed threat actors to compromise the underlying, non-public facing, database server containing the PII and PHI at issue in this case.

[redacted]

[redacted]

E. Threat Actors Sold Class Members' Personal Information on the Dark Web

368. Following the Data Breach, there was evidence that the exfiltrated PII and PHI was available on the dark web and in fact being used to commit fraud.

369. Specifically in November 2018, after forensic evidence proved that files were exfiltrated by threat actors, AMCA was contacted by GlobalOnePay who informed AMCA that [redacted][29] This was done via a "common point of purchase" which is a way for credit card banks to trace fraud associated with the use of their cards.

370. At that time, Conformance Tech noted that there were a [redacted]"[30]

371. In response, [redacted]

[29] [redacted]

[30] AMCAPROD138907.

[31] *Id.*

[32] AMCAPROD0215349.

[redacted]

374. At the end of February 2019, Gemini Advisory, a New York-based company that works with financial institutions to monitor the sale of consumer information on underground markets, ***identified a large number of compromised AMCA patient information for sale on the dark web***.[34] As reported on May 10, 2019 by DataBreaches.net:

> On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs), and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of the American Medical Collection Agency (AMCA), one of the largest recovery agencies for patient collections. Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[35]

375. Gemini's additional research revealed AMCA's exposure window had lasted for at least seven months beginning in September 2018.[36]

376. The combination of AMCA-related PII being for sale on the dark web and the common point of purchase notifications that AMCA received definitively shows that the threat

[33] AMCAPROD1117103.

[34] Gemini Advisory, *AMCA Breach May be Largest Medical Breach in 2019* (June 4, 2019), https://geminiadvisory.io/amca-largest-medical-breach/ (last visited Mar. 21, 2022).

[35] Databreaches.net, *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory* (posted May 10, 2019), https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/ (last visited Mar. 21, 2022).

[36] *Id.*

actors, after exfiltrating PII and PHI from AMCA's systems, sold the information on the dark web and purchasers of that information subsequently committed credit card fraud.

377. On March 1, 2019, Gemini Advisory attempted to notify AMCA of the data exposure, but received no response. Gemini Advisory then contacted federal law enforcement who reportedly followed-up with AMCA.[37]

378. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[38]

379. In its notice to patients affected by the breach, AMCA claims it learned of the unauthorized access on March 20, 2019. Yet Quest failed to take any steps to notify patients whose information was affected until months later, initially only doing so through an SEC filing.

380. There are strong indications that the information exfiltrated from AMCA's database is still being offered for sale on underground markets. A compiled list containing information of more than 60 individuals from varying geographic regions and demographics who had their information stored on AMCA's database was searched across dark web markets notorious for selling confidential personal information acquired from threat actors and malicious threat actors. Of this sample, more than 87% had their information offered for sale by *two single vendors* on just *one* dark web market. It is highly unlikely that information associated with such a significant percentage of the sample would be available through two vendors unless the data was obtained from the same breach—a significant indication that *all* Plaintiffs and Class Members had their information accessed, exfiltrated, and then disseminated by unauthorized parties. Given the

[37] *Id.*

[38] *Id.*

vastness of the dark web, there is high probability that each Plaintiff's and Class Member's data has been disseminated and is available for sale.

F. Quest Announces the Data Breach

381. On June 3, 2019, Quest publicly announced the following in a filing with the SEC:

> On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page. Quest Diagnostics and Optum360 promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access.
>
> Although Quest Diagnostics and Optum360 have not yet received detailed or complete information from AMCA about the incident, AMCA has informed Quest Diagnostics and Optum360 that:
>
> - between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself;
> - the information on AMCA's affected system included financial information (*e.g.*, credit card numbers and bank account information), medical information and other personal information (*e.g.*, Social Security Numbers);
> - as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately 11.9 million people; and
> - AMCA has been in contact with law enforcement regarding the incident.[39]

382. In a written statement attributed to AMCA, AMCA announced that it was still investigating the breach:

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system. Upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page. . . . We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal

[39] Quest Diagnostics Form 8-K, filed June 3, 2019, https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm (last visited Mar. 21, 2022).

> services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information.

383. Although Quest reported that it had only learned of the Data Breach from AMCA on May 14, 2019, the breach was actually discovered at least three months prior to Quest's SEC filing.

384. After Quest's SEC filing, AMCA began sending out notices to those affected by the Data Breach. Quest stated on its website that it had "been advised by AMCA that if your Social Security number or financial information was involved in the incident, you will be notified by letter from AMCA[.]"[40]

385. On June 17, 2019, AMCA filed for Chapter 11 bankruptcy in the Southern District of New York stating an intention to liquidate. The bankruptcy filings describe the types of personal information maintained by AMCA, as well as additional specifics regarding the Data Breach. According to an affidavit submitted by Russell H. Fuchs, the Chief Executive Officer of AMCA:

> [AMCA] by its very nature, requires it to collect and maintain data transmitted to it by its clients that includes personally identifiable information about third-party debtors that could include names, home addresses, Social Security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information. In the case of the AMCA business, that information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought. In all, at any given time, [AMCA] would have held tens of millions of individual points of data regarding millions of individual persons, none of which could be handled without a robust IT system.
>
> [AMCA]'s original IT architecture was built around an IBM mainframe-based system that ran on COBOL4 and served the [AMCA]'s purposes well

[40] Quest Diagnostics, *AMCA Data Security Incident*, https://web.archive.org/web/20200430034243/https://www.questdiagnostics.com/home/AMCA-data-breach-patients/ (last visited Mar. 21, 2022).

> for many years. However, with ever-increasing market demands for enhanced interconnectivity between the [AMCA]'s and its clients' systems, as well as for web-based interaction with both the [AMCA]'s clients and its clients' consumer and patient-debtors, it was clear that continued reliance on the [AMCA]'s internet-unconnected mainframe system would not be tenable in the long term.
>
> Accordingly, in 2015, after several years of internal planning and development, the [AMCA] began to transition to a proprietary, server-based, network-connected system. [AMCA] invested over a million dollars in the new system, employing outside IT consultants to ensure that the system would reflect current technological standards, including, importantly, appropriate data security protocols.[41]

386. AMCA subsequently acknowledged that it "first learned that there might be a problem" when it received a series of common point of purchase notifications that "suggested that a disproportionate number of credit cards that at some point had interacted with the [AMCA's] web portal were later associated with fraudulent charges."[42]

387. In response, AMCA "shut down its web portal to prevent any further compromises of customer data, and engaged outside consultants who were able to confirm that, in fact, [AMCA]'s servers … had been hacked as early as August, 2018." AMCA went on to explain that "the breach required [AMCA] to hire IT professionals and consultants from three different firms, to identify the source of the breach, diagnose its cause, and implement appropriate solutions. To date, these expenses alone cost approximately $400,000, and have effectively shut down outside entry into [AMCA]'s IT network by severely restricting access via the employment of individual authentication mechanisms, VPN access, or specifically vetted 'whitelists' of pre-approved IP's."[43]

---

[41] *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 7:19-bk-23185, ECF No. 2 (Bankr. S.D.N.Y. June 17, 2019).

[42] *Id.*

[43] *Id.*

388. AMCA stated that the costs of providing notice to affected individuals, coupled with the loss of its largest clients LabCorp and Quest, required it to reduce its workforce from 113 employees at year-end 2018 to just 25 employees as of June 17, 2019. As a result, AMCA stated it is "no longer is optimistic that it will be able to rehabilitate its business."[44]

389. Quest and Optum360 had a non-delegable duty to ensure that its systems and those of its vendors and business associates, including AMCA, were sufficient to adequately secure patient information. This was especially true after AMCA transitioned to a "network-connected" system that included "enhanced interconnectivity" and "web-based interaction" between its systems and those of its clients such as Quest and Optum360.

390. By failing to adequately monitor and audit the data security systems of their vendors and business associates, Quest put patient information at severe risk. Following the news that Quest's customers were impacted by the Data Breach, several other labs, who are named as defendants in this action, also announced that their customers had been impacted by the Data Breach.

391. On July 1, 2019, Optum360 disclosed to the Department of Health and Human Services' Office for Civil Rights that 11,500,000 individuals have been affected by the Data Breach.[45]

G. Defendants Failed to Exercise Due Care in Contracting with AMCA, and in Providing More Information than Required to Collect Payments.

392. Defendants failed to exercise reasonable care in protecting patients' information by contracting with AMCA to handle their debt collections.

---

[44] *Id*.

[45] Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 21, 2022).

393. AMCA's bankruptcy filings indicate it was thinly capitalized and had an insignificant IT department with little IT infrastructure. Public reporting has highlighted that AMCA was not a reputable business associate—let alone an associate to be trusted with Plaintiffs' and Class Members' Personal Information.

394. Specifically, AMCA's bankruptcy filings admit that it had less than $4 million in liquidity and its owner had to take a secured personal loan simply to mail notices to those harmed by the Data Breach. Put simply, Quest should not have contracted with an entity that did not even have the means to mail notices to people without having to file for bankruptcy.

395. The length of time between the Data Breach and AMCA's claimed discovery of the Data Breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events were inadequate and not in compliance with industry standards. For example, according to technology security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been trending downward in recent years—due to improvements in detection computer technology.[46] The fact that it took AMCA at least 242 days to detect the Data Breach (and only after being informed by several third parties of ongoing fraud)—nearly 3.5 times the median time for detection in 2018—is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiffs' and Class Members' Personal Information. AMCA's data security deficiencies would have been readily apparent to Quest had it adequately conducted due diligence on AMCA's data security practices before providing AMCA sensitive PHI and PII.

[46] *M-Trends 2019: FireEye Mandiant Services Special Report*, https://content.fireeye.com/m-trends/rpt-m-trends-2019 (last visited March 21, 2022).

396. AMCA's inability to detect its own Data Breach, when an unrelated security firm (Gemini Advisory) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data-security practices, and that Quest failed in its independent obligation to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures. The FireEye report indicates that in 2018, the median amount of time that it took a third-party to detect a data breach was three times the median time for internal detection.[47]

397. AMCA did not need access to Plaintiffs' PHI to collect payments. Instead, AMCA only needed the name of the vendor (Quest), the invoice number, amount owed, and date of service to perform its collection services. But Defendants nevertheless regularly provided full account information that included PHI, apparently because it was more expedient than providing the narrower data set to AMCA.

398. AMCA maintained PHI and PII for closed files and failed to routinely destroy or archive inactive records. Defendants would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by AMCA.

399. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards of PCI DSS.

400. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card

[47] *Id.*

to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[48]

401. Quest had an obligation to exercise oversight over AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could affect Quest's patients. For example, AMCA pointed to the fact that it learned of the unauthorized access in March 2019 through a series of CPP notices suggesting that a "disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges." However, Quest did not learn of the unauthorized access until months later in May 2019.

H. Defendants Failed To Provide Proper Notice Of The Data Breach

402. Although Quest was on actual notice of the Data Breach on May 14, 2019 (and should have known about the Data Breach months earlier), it took until June 3, 2019, to publicly acknowledge the breach and months longer to provide notice to impacted customers.

403. On June 3, 2019, Quest publicly acknowledged the Data Breach and indicated that it would be "working with Optum360 to ensure that Quest patients are appropriately notified consistent with the law."[49]

[48] Securing Account Data with the PCI Point –to-Point Encryption Standard v2, https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last visited Mar. 21, 2022).

[49] Quest Diagnostics Statement on the AMCA Data Security Incident, https://newsroom.questdiagnostics.com/AMCADataSecurityIncident (last visited Mar. 21, 2022).

404. However, rather than sending notice directly, Quest relied on AMCA to mail notices to those individuals on its system in June 2019.[50] The notices provided by AMCA were deficient in several respects. First, AMCA's notices failed to indicate to Quest's customers that it was Quest who had given their information to AMCA. Thus, many affected individuals were left to guess why AMCA had their Personal Information in the first instance. Additionally, the notices failed to inform Quest's customers exactly what information had been accessed, thus preventing them from taking measures that could possibly prevent further harm.

405. It was not until July 8, 2019, almost four months after AMCA received CPP notices, and one month after Quest's first public statement, that Quest put detailed information on its own website regarding the Data Breach and offered credit monitoring to certain affected individuals.[51] But even this effort was deficient in many respects.

a. First, the website indicates that AMCA was the party responsible for sending notice and does not detail any oversight taken by Quest over its business associate.

b. Second, the website limits "complimentary credit monitoring" to those "persons whose Social Security Numbers, credit card information or bank account numbers may have been involved."[52] This limitation means that customers who had other forms of Personal Information taken are not protected. As detailed *infra*, the theft of various forms of Personal Information, not just Social Security Numbers, credit card information, and bank account numbers, can lead to identity theft.

---

[50] Quest Diagnostics: July 8, 2019 Notice Unauthorized Access to Database at AMCA Containing Personal Information, https://web.archive.org/web/20200430034243/https://www.questdiagnostics.com/home/AMCA-data-breach-patients/ (last visited Mar. 21, 2022).

[51] *Id.*

[52] *Id.*

c. Third, Quest acknowledges that there may have been out-of-date contact information for some of its customers. However, Quest provided no means for these customers to obtain information about whether they had been breached and to access credit monitoring. For example, Quest's website does not have any information that its customers can use to determine whether their information was part of the Data Breach.

d. Fourth, Quest's website offered a toll free number that was only available during business hours and for 90 days beginning on July 8, 2019 to allow individuals to "ask questions and learn additional information."[53] This is deficient because (i) the toll-free number and website was only available for a very short period of time; (ii) the website provides no information about what "questions" or "additional information" can be asked or learned; and (iii) the phone number and website are buried in the website's text, without any emphasis, and under a vague "What We Are Doing" heading and much later under a "For More Information" heading.

e. Fifth, the website provides no information about the credit monitoring that Quest purported to offer. Rather, it appears to have only been included in some of the mailings and there is no indication to Quest customers on Quest's website of how to sign up for this service or any other relevant details.

406. Further, data breach letters sent by AMCA and Quest to Quest patients further demonstrate the failure to provide proper notice.

a. First, Quest relied on AMCA to provide "24 months of complimentary credit monitoring and identity theft mitigation services." However, providing a clear end point in

[53] *Id.*

coverage allows threat actors to simply wait out the two years of credit monitoring and then use the stolen information to commit fraud.

b. Second, neither letter specifically informs patients of what information of theirs was taken. AMCA's letter was limited in its specificity to say: "certain other medical information" was taken. Quest fares little better when it tells patients that the information "may have included . . . information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing-and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

c. Third, Quest's letters did not provide the activation code or even reference that patients could receive the 24 months of complimentary credit monitoring. Patients who only received Quest's letter or went to Quest's website would have no idea that they could receive complimentary credit monitoring.

d. Fourth, Quest should not have relied on AMCA—a bankrupt entity—to be the one to cover credit monitoring costs. It is unclear based on available information whether AMCA can fund the complimentary credit monitoring.

407. In sum, Quest's failure to properly disseminate notice further harmed its customers by keeping them in the dark about whether their information was accessed as a result of the Data Breach, what information was accessed as a result of the breach and how they could quickly and safely respond in order to protect themselves from potential harm as a result of the data breach.

I. Defendants Violated HIPAA's Requirements to Safeguard Data and Regulatory Guidance

408. Defendants failed to maintain the privacy and security of their patients' PHI and failed to inform patients that their Personal Information was disclosed. Indeed, Defendants violated HIPAA by failing to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect Plaintiffs' and the Class Members' Personal Information;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

409. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[54]

410. The FTC's publication *Start With Security: A Guide For Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data. Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion

[54] FTC, *Start With Security: A Guide For Businesses*, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Mar. 21, 2022).

detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[55]

411. Additionally, the FTC recommends that organizations limit access to sensitive data, re-quire complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[56]

412. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[57]

413. Defendants were fully aware of their obligations to implement and use reasonable measures to protect the PII and PHI of Quest's patients but failed to comply with these basic recommendations and guidelines that would have prevented the Data Breach from occurring.

[55] *Id*.

[56] *Id*.

[57] FTC, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 21, 2022).

J. Quest Patients' Personal Information Is Highly Valuable

414. Defendants were or should have been aware that they were collecting highly valuable data, for which Defendants knew or should have known there is an upward trend in data breaches in recent years.[58]

415. The U.S. Department of Health and Human Services, Office for Civil Rights, currently lists the Quest track of the AMCA breach as the second largest healthcare breach reported since 2009.[59] Quest patients are the single largest group impacted by this data breach, exceeding the next lab with impacted patients by over 1.3 million patients.[60]

416. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of threat actors, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[61]

---

[58] Healthcare Data Breach Statistics, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Mar. 21, 2022) ("Our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years.").

[59] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 21, 2022).

[60] *Id.* Optum360 is listed as the "Covered Entity" and as the Business Associate for Quest, the Healthcare Provider. The next highest is LabCorp (which is also an MDL Defendant and listed as a Healthcare Provider) with just over 10 million patients as a result of the AMCA breach.

[61] Reuters, *FBI warns healthcare firms they are targeted by hackers*, Aug. 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Mar.21, 2022).

417. The co-founder of Lastline, a network security provider, said that "[h]ackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[62]

418. Other experts have stated that the Data Breach is at "the intersection of three of the types of data that threat actors most desire: personal identifying information that can be used for identity fraud, information about medical conditions, and financial account information."[63]

419. This same article has asked: "why did a collections agency have all of this information in the first place?" It also questioned why medical information and Social Security Numbers needed to be provided to debt collectors.[64]

420. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet . . . having other information makes the data more valuable and the price higher."[65] Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security

---

[62] Christopher Rowland, *Quest Diagnostics discloses breach of patient records*, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited Mar. 21, 2022).

[63] Scott Ikeda, *Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed*, CPO Magazine, June 11, 2019, https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/ (last visited Mar. 21, 2022).

[64] *Id.*

[65] *Id.*

numbers and other Personal Information directly on various dark web[66] sites making the information publicly available.[67]

421. Healthcare data is especially valuable on the black market. According to one report, a healthcare data record may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[68]

422. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[69]

423. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an

---

[66] The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last visited Mar. 21, 2022).

[67] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 21, 2022); McFarland et al., *The Hidden Data Economy*, at 3, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited Mar. 21, 2022).

[68] *Hackers, Breaches, and the Value of Healthcare Data* (Feb. 2, 2022), https://www.securelink.com/blog/healthcare-data-new-prize-hackers/ (last visited Mar. 21, 2022).

[69] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited Jan. 7, 2022).

individual."[70] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[71]

424. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[72]

K. Defendants Have Harmed Plaintiffs And Class Members By Allowing Anyone To Access Their Information

425. Defendants knew or should have known both that medical information is incredibly valuable to threat actors and that health care data breaches are on the rise. Accordingly, Defendants were on notice for the harms that could ensue if they failed to protect patients' data.

---

[70] *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Mar. 21, 2022).

[71] *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 21, 2022).

[72] *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web* (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited March 21, 2022).

426. Quest, moreover, had previously failed to protect patients' private information. In 2016, Quest allowed an unauthorized third party to access its internal internet application and obtain the protected health information of 34,000 individuals.[73] This data included name, date of birth, lab results, and in some instances, phone numbers.[74] At that time, a company spokesman said that "we're taking it seriously."[75]

427. In February 2020, the United States District Court for the District of New Jersey granted final approval of a settlement related to this 2016 breach allowing for up to a $325 reimbursement for each class member.

428. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number), diagnosis codes, credit and debit card numbers, bank account information, and insurance policy numbers—threat actors have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

429. In fact, many victims of the Data Breach have already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized

[73] Press Release, Quest Diagnostics Provides Notice of Data Security Incident, https://web.archive.org/web/20190804190952/http://ir.questdiagnostics.com/news-releases/news-release-details/quest-diagnostics-provides-notice-data-security-incident?ID=2229113&c=82068&p=irol-newsArticle (last visited Mar. 21, 2022).

[74] *Id.*

[75] Robert Channick, *Quest data breach exposes private health information of 34,000 patients*, Chicago Tribune, Dec. 13, 2016, https://www.chicagotribune.com/business/ct-quest-data-hack-1214-biz-20161213-story.html (last visited Mar. 21, 2022).

access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

430. The PII and PHI exposed in the Data Breach is highly coveted and valuable on underground or black markets—and information tied to this Data Breach has already been offered for sale. For example, identity thieves can use the stolen information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

431. While federal law generally limits an individual's liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[76] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the

[76] *Ponemon Institute, Fifth Annual Study on Medical Identity Theft*, https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 (last visited Mar. 21, 2022).

identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[77]

432. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[78]

433. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[79]

434. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[80] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[81]

435. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing

[77] *Id*. at 9.

[78] *Id*. at 2.

[79] *Id*. at 14.

[80] *Id*. at 1.

[81] *Id*.

medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits ;
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[82]

436. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[83] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[84] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

437. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are

[82] *FTC, Medical Identity Theft FAQs for Health Care Providers and Health Plans*, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited Mar. 21, 2022).

[83] *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited March 21, 2022).

[84] *Id*.

often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[85]

438. As AMCA acknowledged, fraudulent charges have already been linked to the data Quest provided to AMCA. Quest publicly revealed the exposure of patients' Personal Information only after "a disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[86]

439. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[87] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

440. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment – even surgery – or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record.

---

[85] *Id.*

[86] Decl. of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 And In Support Of "First Day" Motions, American Medical Collection Agency Bankruptcy Petition #19-23185(RDD), ECF No. 2 (Bankr. S.D.N.Y.).

[87] Identity Theft Resource Center, *The Aftermath 2017*, https://web.archive.org/web/20200512124018/https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited March 21, 2022).

> It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[88]

441. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts; and

h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

[88] *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, https://web.archive.org/web/20201019075254/https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last visited Mar. 21, 2022).

442. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[89]

443. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[90]

444. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[91]

---

[89] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Mar. 21, 2022).

[90] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), http://www.gao.gov/new.items/d07737.pdf (last visited Mar. 21, 2022).

[91] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Mar. 21, 2022).

445. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendants would have no reason to tout their data security efforts to their actual and potential customers.

446. Consequently, had consumers known the truth about Defendants' data security practices—that they did not adequately protect and store their Personal Information—they would not have entrusted their Personal Information to Quest.

447. Quest's failure to protect Plaintiffs' and Class Members' personal data has led to significant governmental investigation. Specifically, on June 5, 2019, New Jersey's United States Senators Cory Booker and Bob Menendez sent a letter to Quest's Chairman, President & CEO stating that they were "deeply concerned" and asking for detailed information about the breach, Quest's responses, and Quest's data security processes.[92]

448. Separately, the Attorneys General of Connecticut and Illinois opened an investigation on June 7, 2019 into Quest and LabCorp. In a press release, they stated: "The last thing patients should have to worry about is whether their personal information has been compromised by the entities responsible for protecting it. I am committed to ensuring that impacted patients receive timely notification and that the companies involved take precautions to protect consumers' sensitive health and financial information in the future."[93] Michigan's Attorney

[92] Ltr. from U.S. Senators Robert Menendez and Cory A. Booker (June 5, 2019), https://www.menendez.senate.gov/imo/media/doc/06.05.19%20LabCorp%20Letter.pdf (last visited Mar. 21, 2022).

[93] Connecticut and Illinois Open Investigation into Quest Diagnostics, LabCorp Data Breach, The Office of Attorney General William Tong, https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH (last visited Mar. 21, 2022).

General also launched an investigation shortly after the Data Breach was announced.[94] In its quarterly SEC filing, Quest acknowledged that "certain federal and state governmental authorities are investigating, or otherwise seeking information and/or documents from the Company related to the AMCA Data Security Incident and related matters, including Attorneys General offices from numerous states and the District of Columbia and certain U.S. senators."[95]

CLASS ACTION ALLEGATIONS

I. NATIONWIDE CLASS

449. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States whose Personal Information was compromised in the Data Breach.

450. The Nationwide Class asserts claims against Defendants for negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), invasion of privacy – intrusion upon seclusion (Count 4), and unjust enrichment (Count 5).

II. STATEWIDE SUBCLASSES

451. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 6

[94] AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities, HIPPA Journal, https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/ (last visited Mar. 21, 2022).

[95] Quest Diagnostics, Inc. Form 10-Q (Oct. 23, 2019), http://d18rn0p25nwr6d.cloudfront.net/CIK-0001022079/9fd46d10-0cf2-4eb7-9140-c903f6b5c641.pdf (last visited Mar. 21, 2022).

through 23), on behalf of separate statewide subclasses for each State (the "Statewide Subclasses"), defined as follows:

> All natural persons residing in [name of state] whose Personal Information was compromised in the Data Breach.

452. Excluded from the Nationwide Class and each Statewide Subclass are Defendants, any entity in which either Defendant has a controlling interest, and either Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

453. **Numerosity. Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendants have acknowledged that millions of Quest customers' Personal Information has been compromised. Those individuals' names and addresses are available from Defendants' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Statewide Subclass, making joinder of all Statewide Subclass members impracticable.

454. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendants had a duty to protect Personal Information;

b. Whether Defendants failed to take reasonable and prudent security measures;

c. Whether Defendants knew or should have known of the susceptibility of AMCA's systems to a data breach;

d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendants' security measures to protect its systems were reasonable in light known legal requirements;

f. Whether Defendants were negligent in failing to adequately monitor and audit the data security systems of their vendors and business associates;

g. Whether Defendants' efforts (or lack thereof) to ensure the security of patients' Personal Information provided to vendors and business associates were reasonable in light of known legal requirements;

h. Whether Defendants' conduct constituted unfair or deceptive trade practices;

i. Whether Defendants violated state law when they failed to implement reasonable security procedures and practices;

j. Which security procedures and notification procedures Defendants should be required to implement;

k. Whether Defendants have a contractual obligation to use reasonable security measures;

l. Whether Defendants have complied with any contractual obligation to use reasonable security measures;

m. What security measures, if any, must be implemented by Defendants to comply with their contractual obligations;

n. Whether Defendants violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

o. Whether Defendants failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;

p. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of AMCA's systems and/or the loss of the Personal Information of Plaintiffs and Class Members;

q. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Personal Information; and,

r. Whether Plaintiffs and Class Members are entitled to damages or injunctive relief.

455. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

456. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in

litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

457. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

458. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendants or would be dispositive of the interests of members of the proposed Class.

459. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. The Class and Subclasses consist of individuals who received services from Quest and whose accounts were placed into collections with AMCA by Quest. Class Membership can be determined using Quest and AMCA's records in their databases.

460. **Injunctive Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

461. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Defendants failed to adequately monitor and audit the data security systems of their vendors and business associates;

d. Whether Defendants were unfairly and unjustly enriched as a result of their improper conduct, such that it would be inequitable for Defendants to retain the benefits conferred upon them by Plaintiffs and the other Class Members;

e. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

462. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

463. Quest required Plaintiffs and Class Members to submit Personal Information to obtain diagnostic and medical services, which Quest provided to Optum360 and its vendor AMCA for billing purposes. Defendants collected and stored the Personal Information for commercial gain.

464. Defendants knew or should have known that AMCA's systems were vulnerable to unauthorized access and exfiltration by third parties.

465. Defendants had a non-delegable duty to ensure that contractual partners with whom they shared patient information maintained adequate and commercially reasonable data security practices to ensure the protection of patients' Personal Information.

466. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

467. Defendants owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

468. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendants with their confidential data as part of the health treatment process. Only Defendants were in a position to ensure that their contractual partners had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

469. Defendants' duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as their own promises regarding privacy and data security to Quest's patients. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiffs' and Class Members' information from threat actors.

470. Defendants' duties also arose under HIPPA regulations, which, as described above, applied to Defendants and establish national standards for the protection of patient information, including protected health information, which required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy Rule

requirement that Defendants obtain satisfactory assurances from their business associate AMCA that AMCA would appropriately safeguard the protected health information it receives or creates on behalf of the Defendants. 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

471. Defendants' duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

472. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its vendors and business associates' systems, and the importance of adequate security. Quest specifically knew about the risks inherent in collecting and storing Personal Information given its experience with a recent cyber-attack in November 2016 and its acknowledgment that Quest's "business associates" are "required to maintain the privacy and security of [patients'] PHI."

473. Defendants breached their common law, statutory, and other duties – and thus were negligent – by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

474. Defendants breached their duties to Plaintiffs and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit the data security systems of its vendors and business associates;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

475. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

476. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Personal Information.

477. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as described in this Complaint.

478. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information.

479. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

COUNT 2

NEGLIGENCE PER SE
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

480. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

481. Defendants are entities covered by HIPAA (45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"),

and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

482. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendants to obtain satisfactory assurances that its business associates would appropriately safeguard the protected health information it receives or creates on behalf of the Defendants. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. AMCA constitutes a "business associate" within the meaning of HIPAA.

483. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiff and Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

484. Defendants violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' Personal Information, as described herein.

485. Defendants' violations of HIPAA constitute negligence per se.

486. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

487. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

488. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

489. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

490. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Quest, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

491. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

492. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

493. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

494. As a direct and proximate result of Defendants' negligence per se under HIPAA and the FTC Act, Plaintiffs and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

BREACH OF CONFIDENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

495. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

496. Plaintiffs and Class Members maintained a confidential relationship with Defendants whereby Defendants undertook a duty not to disclose the Personal Information provided by Plaintiffs and Class Members to Defendants to unauthorized third parties. Such Personal Information was confidential and novel, highly personal and sensitive, and not generally known.

497. Defendants knew Plaintiffs' and Class Members' Personal Information was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the Personal Information they collected, stored, and maintained.

498. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' Personal Information in violation of this understanding. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the Personal Information in their possession and failed to comply with industry-standard data security practices.

499. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

500. As a direct and proximate result of Defendants' breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT 4

INVASION OF PRIVACY – INTRUSION UPON SECLUSION
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

501. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

502. Defendants intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their Personal Information to a third party that was unequipped and unable to keep their Personal Information secure.

503. By failing to keep Plaintiffs' and Class Members' Personal Information secure, and disclosing Personal Information to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, *inter alia*:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their Personal Information from disclosure to unauthorized persons; and

d. enabling the disclosure of their Personal Information without consent.

504. The Personal Information that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, health, and treatment information.

505. As a direct and proximate result of Defendants' intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein.

Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT 5

UNJUST ENRICHMENT[96]
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

506. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

507. For years and continuing to today, Defendants' business model has depended upon patients entrusting them with their Personal Information. Trust and confidence are critical and central to both the services provided by Quest to patients and the billing and collection for such services. Unbeknownst to Plaintiffs and Class Members, however, Defendants failed to ensure their vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' and Class Members' Personal Information. Defendants' deficiencies described herein were contrary to their security messaging.

508. Plaintiffs and Class Members engaged Quest for services and provided Defendants with, and allowed Defendants to collect, their Personal Information on the mistaken belief that Defendants complied with their duty to safeguard and protect patients' Personal Information. Putting their short-term profit ahead of safeguarding Personal Information, and unbeknownst to Plaintiffs and Class Members, Defendants knowingly sacrificed security in favor of collecting moneys Defendants believed they were owed. Defendants knew that the manner in which they maintained and transmitted patients' Personal Information violated their fundamental duties to

[96] Plaintiffs recognize the Court's order holding that Plaintiffs failed to state an unjust enrichment claim on the grounds that "there is no [] allegation that Defendants . . . receive any additional value from Plaintiffs Personal Information." ECF No. 283 at 33-34. Plaintiffs have added additional allegations to this Count to address this holding and otherwise assert it to preserve it for appeal.

Plaintiffs and Class Members by disregarding industry-standard security protocols to ensure confidential information was securely transmitted and stored.

509. Defendants had within their exclusive knowledge at all relevant times the fact that their vendors and business associates failed to implement adequate security measures to keep patients' Personal Information secure. This information was not available to Plaintiffs, Class Members, or the public at large.

510. Defendants also knew that Plaintiffs and Class Members expected that their information would be kept secure against known security risks and that the security protocols of any vendors or business associates used by Defendants would be thoroughly vetted before they received patients' Personal Information. And based on this expectation and trust, Defendants knew that Plaintiffs and Class Members would not have disclosed health information to it and would have chosen a different provider for services.

511. Plaintiffs and Class Members did not expect that Defendants would store or transmit their Personal Information insecurely or engage a billing collection agency, AMCA, that employed substantially deficient security protocols and would store highly sensitive PHI that was irrelevant to collecting payments.

512. Had Plaintiffs and Class Members known about Defendants' practice of sharing their Personal Information with vendors and business associates who were unequipped to protect it and insecurely transmitting sensitive PHI that had no bearing on collecting payments, Plaintiffs and Class Members would not have engaged Defendants to perform any services and would never have provided Defendants with their Personal Information.

513. By withholding these material facts, Defendants put their own interests ahead of their patients' interests and benefitted themselves to the detriment of Plaintiffs and Class Members.

514. As a result of their conduct as alleged herein, Defendants sold more services than they otherwise would have and were able to charge Plaintiffs and Class Members when they otherwise could not have. Defendants were unjustly enriched by charging and collecting for those services to the detriment of Plaintiffs and Class Members.

515. To be sure, this is not a question of whether Defendants misused patients' Personal Information to collect payment for services already provided. It is more foundational. Defendants promised to protect and safeguard Plaintiffs' and Class Members' Personal Information at all times (from the inception of their relationship of trust and confidence) and never would have performed any services of value enabling them to bill or collect payment but for Defendants' unfair and deceptive practices.

516. It would be inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

517. Defendants' defective security and their unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their private Personal Information.

518. Each Plaintiff and member of the proposed Classes is entitled to restitution and non-restitutionary disgorgement in the amount by which Defendants were unjustly enriched, to be determined at trial.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 6

CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code §§ 56, *et seq.*

519. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

520. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.*

521. The CMIA further requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

522. Plaintiff and California Subclass members are "patient[s]," "whether or not still living, who received health care services from a provider of health care and to whom medical information pertains" pursuant to § 56.05(k) of the CMIA.

523. Defendants are each a "provider of healthcare" pursuant to § 56.05(m) of the CMIA "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information."

524. Defendants are subject to the requirements and mandates of the CMIA and are therefore required to do the following under the CMIA:

a. Ensure that medical information regarding patients is not disclosed or disseminated or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101;

b. Not disclose medical information regarding a patient without first obtaining an authorization under Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35 and 56.104;

c. Create, maintain, preserve, and store medical records in a manner that preserves the confidentiality of the information contained therein under Cal. Civ. Code §§ 56.06 and 56.101(a);

d. Protect and preserve confidentiality of electronic medical information in their possession under Cal. Civ. Code §§ 56.06 and 56.101(b)(1)(A); and

e. Take appropriate preventive actions to protect confidential information or records from unauthorized release under Cal. Civ. Code § 56.36I(2)(E).

525. The Personal Information of Plaintiff and California Subclass members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

526. The medical information compromised included Plaintiff's and California Subclass members' full names, mailing addresses, phone numbers, email addresses, dates of birth, Social Security numbers, and genders, in conjunction with information related to Plaintiff's and California Subclass members' medical treatment, such as physician names, dates of service, names

of labs, test names, internal patient identification numbers, insurance information, and other diagnosis and test codes, including ICD Codes that represent specific conditions, diseases, medical history, mental and physical conditions, and treatments associated with those code that can be quickly and easily referenced online and elsewhere. This information considered in its totality constitutes individually identifiable information regarding a patient's medical history, mental or physical condition, and/or treatment.

527. Due to Defendants' negligent creation, maintenance, preservation and/or storage of Plaintiff's and the California Subclass members' electronic medical information, Defendants allowed Plaintiff's and California Subclass members' individually identifiable medical information to be accessed and actually viewed by at least one unauthorized third party, constituting a release in violation of Cal. Civ. Code § 56.101(b)(1)(A).

528. Defendants disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). Plaintiff and California Subclass members did not authorize Defendants' disclosure and release of their Personal Information that occurred in the Data Breach.

529. Defendants' negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and the California Subclass members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA, Cal. Civ. Code §§ 56.06 and 56.101(a). Defendants transmitted patients' confidential medical information in an unencrypted and unredacted format to Defendants' associates which was then accessed, viewed, and exfiltrated by an unauthorized third party or parties, and thus Defendants negligently released medical information concerning Plaintiff and California Subclass members. Accordingly,

Defendants' systems and protocols did not protect and preserve the integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code § 56.101.

530. Defendants violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiff's and California Subclass members' Personal Information; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and California Subclass members' Personal Information and ensuring their vendors and business associates implemented such measures; (3) failing to use reasonable authentication procedures to track Personal Information in case of a security breach and ensuring their vendors and business associates implemented such measures; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiff's and California Subclass members' Personal Information was kept.

531. Defendants' failure to implement adequate data security measures to protect the Personal Information of Plaintiff and California Subclass members was a substantial factor in allowing unauthorized parties to access AMCA's computer systems and acquire the Personal Information of Plaintiff and California Subclass members.

532. As a direct and proximate result of Defendants' violation of the CMIA, Defendants allowed the Personal Information of Plaintiff and California Subclass members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and/or profit from their Personal Information, thereby breaching the confidentiality

of their Personal Information. Plaintiff and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

533. Plaintiff and California Subclass members were injured and have suffered damages, as described above, from Defendants' unauthorized release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and are therefore entitled to nominal damages of one thousand dollars ($1,000) for each violation under Civil Code §56.36(b)(1) or the amount of actual damages, if any, for each violation under Civil Code §56.36(b)(2).

534. Plaintiff and California Subclass members also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23, Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

COUNT 7

CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §§ 17200, *et seq.*

On Behalf of the California Subclass against Defendant Quest

535. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

536. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

537. Defendant violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

538. Defendant's "unfair" and "fraudulent" acts and practices include omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and California Subclass members' Personal Information.

539. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, HIPAA, and California common law.

540. Defendant engaged in acts of deception and false pretense in connection with its accepting, collecting, securing, and otherwise protecting patient Personal Information and engaged in the following deceptive and unconscionable trade practices, including:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit the data security systems of its vendors and business associates;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

541. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and unfair breach of its duties.

542. Defendant's failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Personal Information.

543. Plaintiff and California Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions and deceptive, unfair, and unlawful practices. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and California Subclass members would not have sought or purchased services from Defendant.

544. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein.

545. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their Personal Information; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 8

CALIFORNIA CONSUMER LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq.*
On Behalf of the California Subclass against Defendant Quest

546. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

547. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

548. Defendant is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

549. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

550. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

551. Plaintiff and California Subclass members are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

552. Defendant's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including, but not limited to omitting, suppressing, and concealing the material fact that it

did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and California Subclass members' Personal Information.

553. Defendant's omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

554. Plaintiff and California Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and California Subclass members would not have sought or purchased services from Defendant.

555. Had Defendant disclosed to Plaintiffs and Class members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and California Subclass members' Personal Information as part of the services they provided without advising Plaintiffs and California Subclass members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and California Subclass members' Personal Information. Accordingly, Plaintiff and California Subclass members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered.

556. As a direct and proximate result of Defendant's violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

557. Plaintiff and California Subclass members have provided notice of their claims for damages to Defendant, in compliance with California Civil Code § 1782(a).

558. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 9

INDIANA UNFAIR TRADE PRACTICES ACT
Indiana Code § 24-5-0.5
On Behalf of the Indiana Subclass against Defendant Quest

559. The Indiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, restate and re-allege the preceding paragraphs as if fully set forth herein.

560. Defendant is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

561. Defendant is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

562. Defendant engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

563. Defendant engaged in unfair, abusive, and deceptive acts, and practices, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Indiana Subclass members' Personal Information.

564. Defendant's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

565. The injury to consumers from Defendant's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

566. Consumers could not have reasonably avoided injury because Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Defendant created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

567. Defendant's inadequate data security had no countervailing benefit to consumers or to competition.

568. Defendant's acts and practices were "abusive" for numerous reasons, including:

a. because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Defendant's failure to disclose the inadequacies in their data security interfered with consumers' decision-making in a variety

of their transactions.

b. because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Defendant's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Defendant concerning the state of Defendant's' security.

d. because Defendant took unreasonable advantage of consumers' reasonable reliance that they were acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed four paragraphs below.

569. Defendant also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including failing to disclose that it did not review and monitor the adequacy of its business associates' data security practices.

570. Defendant intended to mislead Plaintiff and Indiana Subclass members and induce them to rely on its omissions.

571. Plaintiff and Indiana Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Indiana Subclass members would not have sought or purchased services from Defendant.

572. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

573. Defendant had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the Personal Information in their possession. This duty arose because members of the public, including Plaintiff and the Indiana Subclass, repose a trust and confidence in Defendants to keep their Personal Information secure. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of its vendors' and business associates' systems; and

b. Active concealment of the state of AMCA's security.

574. Defendant acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass members' rights. Defendant's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

575. Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 on November 14, 2019. Defendant has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

576. Defendant's conduct includes incurable deceptive acts that Defendant engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

577. As a direct and proximate result of Defendant's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

578. Defendant's violations present a continuing risk to Plaintiff and Indiana Subclass members as well as to the general public.

579. Plaintiff and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 10

PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, Iowa Code § 715C.2

580. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

581. Defendants are each "persons" as defined by Iowa Code § 715C.2(10).

582. Plaintiffs are each "consumers" as defined by Iowa Code § 715C.2(2).

583. Defendants are each business that own or license computerized data that includes Personal Information as defined by Iowa Code § 715C.2(1).

584. Plaintiff's and Iowa Subclass members' Personal Information includes Personal Information as covered under Iowa Code § 715C.2(1).

585. Defendants are required to accurately notify Plaintiff and Iowa Subclass members if they become aware of a breach of their data security systems in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

586. Because Defendants were aware of a breach of their vendor AMCA's security system involving the Personal Information of Plaintiff and Iowa Subclass members that Defendants provided to AMCA, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

587. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Iowa Code § 715C.2(1).

588. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

589. As a direct and proximate result of Defendants' violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as described above.

590. Plaintiff and Iowa Subclass members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

COUNT 11

IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT, Iowa Code § 714H

On Behalf of the Iowa Subclass against Defendant Quest

591. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

592. Defendant is a "person" as defined by Iowa Code § 714H.2(7).

593. Plaintiff and Iowa Subclass members are "consumers" as defined by Iowa Code § 714H.2(3).

594. Defendant's conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

595. Defendant engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Iowa Subclass members' Personal Information.

596. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

597. Defendant intended to mislead Plaintiff and Iowa Subclass members and induce them to rely on its omissions.

598. Plaintiff and Iowa Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing

collector AMCA adequately secured patients' Personal Information, Plaintiff and Iowa Subclass members would not have sought or purchased services from Defendant.

599. As a direct and proximate result of Defendant's unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

600. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

601. Plaintiff and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 12

PROTECTION OF CONSUMER INFORMATION
Kan. Stat. Ann. §§ 50-7a02(a), *et seq*.

602. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

603. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

604. Plaintiff's and Kansas Subclass members' Personal Information includes Personal Information as covered under Kan. Stat. Ann. § 50-7a02(a).

605. Defendants are required to accurately notify Plaintiffs and Kansas Subclass members if they become aware of a breach of their data security systems that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

606. Because Defendants were aware of a breach of their vendor AMCA's security system involving the Personal Information of Plaintiff and Kansas Subclass members that Defendants provided to AMCA and that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

607. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Kan. Stat. Ann. § 50-7a02(a).

608. As a direct and proximate result of Defendants' violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

609. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT 13

KANSAS CONSUMER PROTECTION ACT,
K.S.A. §§ 50-623, *et seq.*
On Behalf of the Kansas Subclass against Defendant Quest

610. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

611. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

612. Plaintiff and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

613. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

614. Defendant is a "supplier" as defined by K.S.A. § 50-624(l).

615. Defendant advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

616. Defendant engaged in deceptive and unfair acts or practices, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kansas Subclass members' Personal Information.

617. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

618. Defendant intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its omissions.

619. Plaintiff and Kansas Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Kansas Subclass members would not have sought or purchased services from Defendant.

620. Defendant also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and Kansas Subclass members to reasonably protect their interests, due to their lack of knowledge, K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and Kansas Subclass members to enter into a consumer transaction on terms that Defendant knew was substantially one-sided in favor of Defendant, K.S.A. § 50-627(b)(5)).

621. Plaintiff and Kansas Subclass members had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Defendant's possession.

622. The above unfair, deceptive, and unconscionable practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

623. As a direct and proximate result of Defendant's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

624. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; restitution; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 14

KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT, Ky. Rev. Stat. Ann. §§ 365.732, *et seq.*

625. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

626. Defendants are each a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

627. Plaintiff's and Kentucky Subclass members' Personal Information includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

628. Defendants are required to accurately notify Plaintiff and Kentucky Subclass members if they become aware of a breach of their data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members'

Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

629. Because Defendants were aware of a breach of their vendor AMCA's security system involving the Personal Information of Plaintiff and Kentucky Subclass members that Defendants provided to AMCA that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

630. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Ky. Rev. Stat. Ann. § 365.732(2).

631. As a direct and proximate result of Defendants' violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass members suffered damages, as described above.

632. Plaintiff and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

COUNT 15

KENTUCKY CONSUMER PROTECTION ACT, Ky. Rev. Stat. §§ 367.110, *et seq.*
On Behalf of the Kentucky Subclass against Defendant Quest

633. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, restate and re-allege the preceding paragraphs as if fully set forth herein.

634. Defendant is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

635. Defendant advertised, offered, or sold goods or services in Kentucky and engaged in "trade" or "commerce" directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

636. Defendant engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kentucky Subclass members' Personal Information.

637. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

638. Plaintiff and Kentucky Subclass members purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Defendant's unlawful acts and practices.

639. Plaintiff and Kentucky Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Kentucky Subclass members would not have sought or purchased services from Defendant.

640. The above unlawful acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

641. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiff and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

642. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 16

MICHIGAN CONSUMER PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.903, *et seq*. On Behalf of the Michigan Subclass against Defendant Quest

643. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

644. Defendant and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

645. Defendant advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g)

646. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors

and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass members' Personal Information.

647. Plaintiff and Michigan Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Michigan Subclass members would not have sought or purchased services from Defendant.

648. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

649. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, restitution, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT 17

MINNESOTA CONSUMER FRAUD ACT,
Minn. Stat. §§ 325F.68, *et seq*. and Minn. Stat. §§ 8.31, *et seq.*
On Behalf of the Minnesota Subclass against Defendant Quest

650. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

651. Defendant, Plaintiff, and Minnesota Subclass members are each a "person" as defined by Minn. Stat. § 325F.68(3).

652. Defendant's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

653. Defendant engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

654. Defendant engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Minnesota Subclass members' Personal Information.

655. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

656. Plaintiff and Minnesota Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure

its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Minnesota Subclass members would not have sought or purchased services from Defendant.

657. Defendant's fraudulent, misleading, and deceptive practices affected the public interest, including those affected by the Data Breach.

658. As a direct and proximate result of Defendant's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

659. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT 18

MISSOURI MERCHANDISING PRACTICES ACT, Mo. Rev. Stat. §§ 407.010, *et seq.*
On Behalf of the Missouri Subclass against Defendant Quest

660. The Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

661. Defendant is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

662. Defendant advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

663. Defendant engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Missouri Subclass members' Personal Information.

664. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

665. Plaintiff and Missouri Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Missouri Subclass members would not have sought or purchased services from Defendant.

666. As a direct and proximate result of Defendant's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for

fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

667. Plaintiff and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS

COUNT 19

NOTICE OF SECURITY BREACH
N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq.*

668. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

669. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

670. Plaintiff's and New Hampshire Subclass members' Personal Information includes Personal Information as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

671. Defendants are required to accurately notify Plaintiff and New Hampshire Subclass members if Defendants become aware of a breach of their data security systems in which misuse of Personal Information has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

672. Because Defendants were aware of a security breach of AMCA's security systems involving the Personal Information of Plaintiff and New Hampshire Subclass members that Defendants provided to AMCA and in which misuse of Personal Information has occurred or is

reasonably likely to occur, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

673. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

674. As a direct and proximate result of Defendants' violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass members suffered damages, as described above.

675. Plaintiff and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including actual damages and injunctive relief.

COUNT 20

NEW HAMPSHIRE CONSUMER PROTECTION ACT, N.H.R.S.A. §§ 358-A, *et seq.*

On Behalf of the New Hampshire Subclass against Defendant Quest

676. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

677. Defendant is a "person" under the New Hampshire Consumer Protection Act.

678. Defendant advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1.

679. Defendant engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and New Hampshire Subclass members' Personal Information.

680. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information. Defendant's acts and practices went beyond the realm of strictly private transactions.

681. Plaintiff and New Hampshire Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and New Hampshire Subclass members would not have sought or purchased services from Defendant.

682. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and New Hampshire Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

683. Plaintiff and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 21

NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J.S.A. §§ 56:8-163, *et seq.*

On Behalf of the New Jersey Subclass against Defendant Optum360

684. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

685. Defendant is a business that conducts business in New Jersey under N.J.S.A. § 56:8-163(a).

686. Plaintiff's and New Jersey Subclass members' Personal Information includes Personal Information covered under N.J.S.A. §§ 56:8-163, *et seq.*

687. Under N.J.S.A. § 56:8-163(a), "[a]ny business that conducts business in New Jersey. . . shall disclose any breach of security of [] computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

688. Because Defendant discovered a breach of AMCA's security system involving the Personal Information of Plaintiff and New Jersey Subclass members that Defendant provided to AMCA in which such Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J.S.A. §§ 56:8-163, *et seq.*

689. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated N.J.S.A. § 56:8-163(a).

690. As a direct and proximate result of Defendant's violations of N.J.S.A. § 56:8-163(a), Plaintiff and New Jersey Subclass members suffered the damages described above.

691. Plaintiff and New Jersey Subclass members seek relief under N.J.S.A. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 22

NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.*
On Behalf of the New York Subclass against Defendant Quest

692. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

693. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and New York Subclass members' Personal Information.

694. Plaintiff and New York Subclass members were deceived in New York. They also transacted with Defendants in New York by utilizing Defendant's services in New York.

695. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

696. Plaintiff and New York Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure

its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and New York Subclass members would not have sought or purchased services from Defendant.

697. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

698. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the hundreds of thousands, if not millions, of New Yorkers affected by the Data Breach.

699. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

700. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 23

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*

On Behalf of the Pennsylvania Subclass against Defendant Quest

701. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

702. Defendants is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

703. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

704. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Pennsylvania Subclass members' Personal Information.

705. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

706. Plaintiff and Pennsylvania Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Pennsylvania Subclass members would not have sought or purchased services from Defendant.

707. Defendant acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights.

708. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

709. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

REQUESTS FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully requests that the Court enter judgment in their favor and against Defendants, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

7. That the Court award pre- and post-judgment interest at the maximum legal rate; and

8. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

SEEGER WEISS LLP
Quest Track Co-Lead Counsel

By:/s/ Christopher A. Seeger
CHRISTOPHER A. SEEGER

Dated: March 31, 2022

Christopher A. Seeger
Christopher Ayers
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, New Jersey 07660
(973) 639-9100

E. Michelle Drake
BERGER MONTAGUE PC
43 SE Main Street, Suite 505
Minneapolis, Minnesota 55414
(612) 594-5999

Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100

Jason L. Lichtman
Sean A. Petterson
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, New York 10013
(212) 355-9500

Quest Track Co-Lead Counsel

James E. Cecchi
CARELLA BYRNE CECCHI OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700

Lead Counsel for Plaintiffs

Jason T. Dennett
Kim D. Stephens
Cecily C. Shiel
TOUSLEY BRAIN STEPHENS, PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
(206) 682-5600

Timothy G. Blood
Thomas J. O'Reardon II
BLOOD HURST & O'REARDON, LLP
502 West Broadway, Suite 1490
San Diego, California 92101
(619) 338-1101

Todd S. Garber
Jeremiah Frei-Pearson
D. Greg Blankinship
Chantal Khalil
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
445 Hamilton Avenue, Suite 605
White Plains, New York 10601
(914) 298-3281

Quest Track Steering Committee